Cisco Self Defending Network

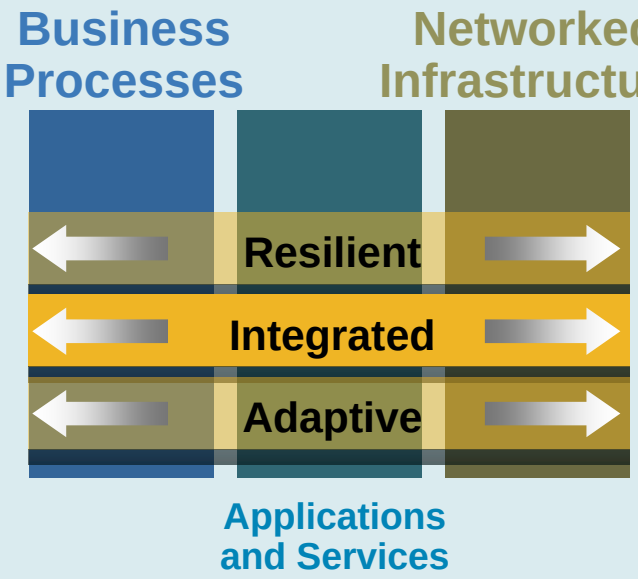
Mai 2007

Intelligent Networking
Using the Network to Enable Business Processes

Cisco Network Strategy

Utilize the Network to Unite Isolated Layers and Domains to Enable Business Processes

Connectivity



Intelligent Networking

- **Active participation** in application and service delivery
- **A systems approach** integrates technology layers to reduce complexity
- Flexible **policy controls** adapt this intelligent system to your business though business rules

When it comes to information security, what are the objectives?

- Align security practice and policy to business requirements. Security that's a business enabler, not an inhibitor.
- Keep costs appropriate: It's not necessarily about reducing costs, but rather, spending where it counts the most
- Reduce complexity of the overall environment
- Control and contain threats so they don't control you

- The network touches all parts of the infrastructure
- It is uniquely positioned to help solve these issues

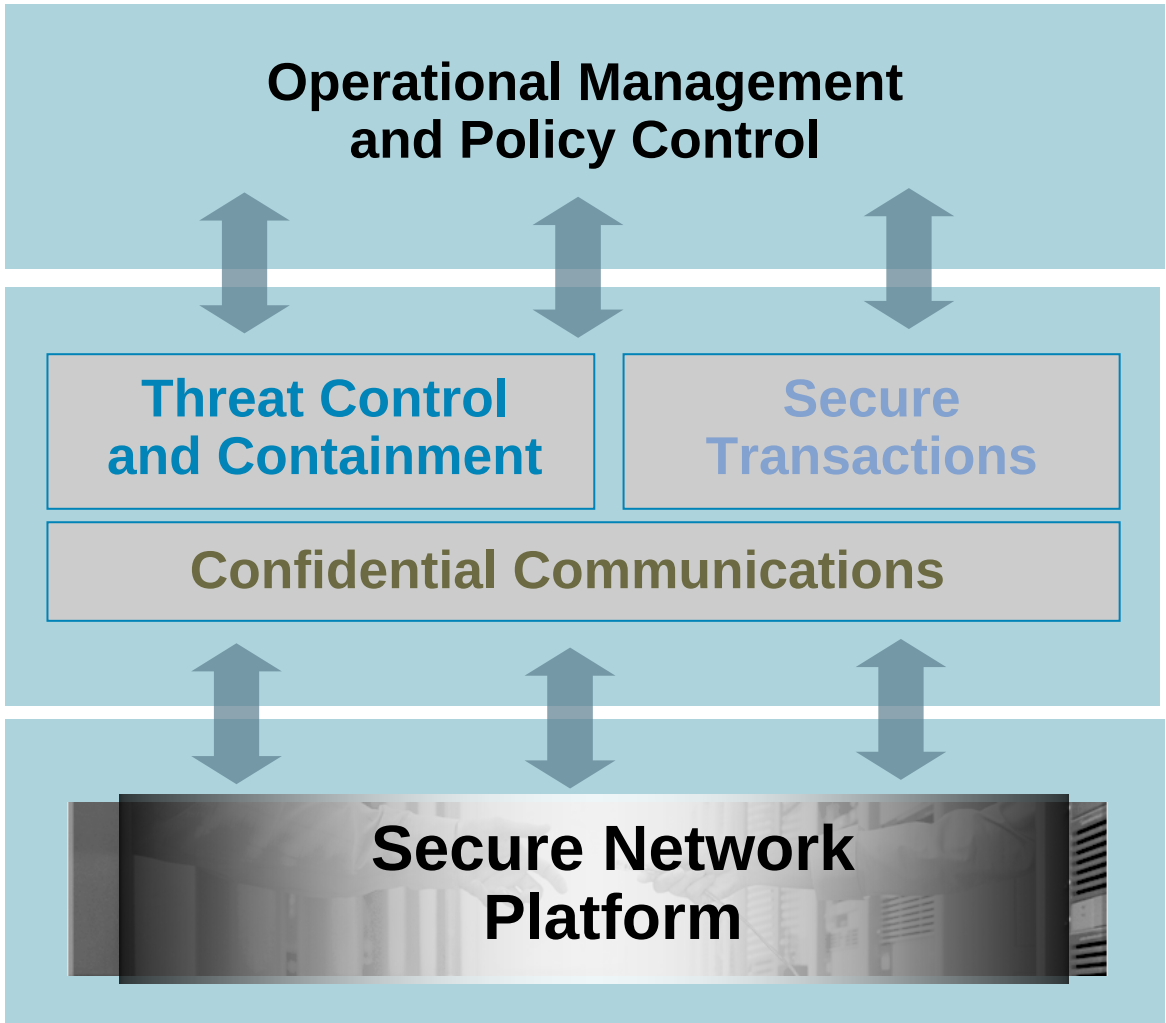
Self-Defending Network Defined

Efficient Security Management, Control, and Response

Advanced technologies and security services to

- **Mitigate the effects of outbreaks**
- **Protect critical assets**
- **Ensure privacy**

Network as Platform



Self-Defending Network – "*Le réseau peut identifier, s'adapter et répondre aux attaques*"

Succursale

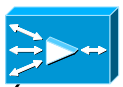
Les 3 Pilliers du SDN:

Intégration

Collaboraton

Réaction

MARS & CSM



WAAS

Wan avec chiffrement

"Distribution automatique des signatures"

Détection D'Intrusion

Routeur ISR

FW

IPS

VPN

Pare-Feu

ASA

FW

VPN

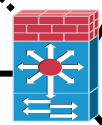
IPS

Anti-X

Prévention d'Intrusion

Cisco NAC

WAAS



Commutateurs

SONA

PCs

CSA – Cisco Security Agent

Serveurs

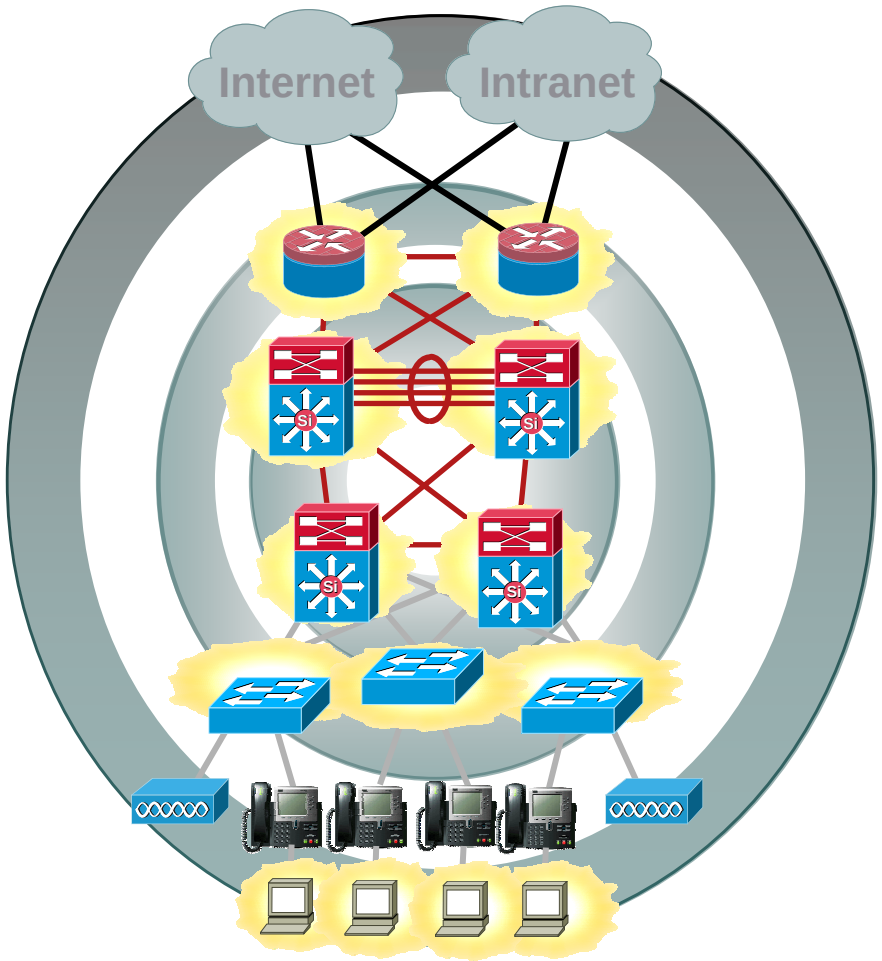
CSA

"Vision limitée, précision limitée

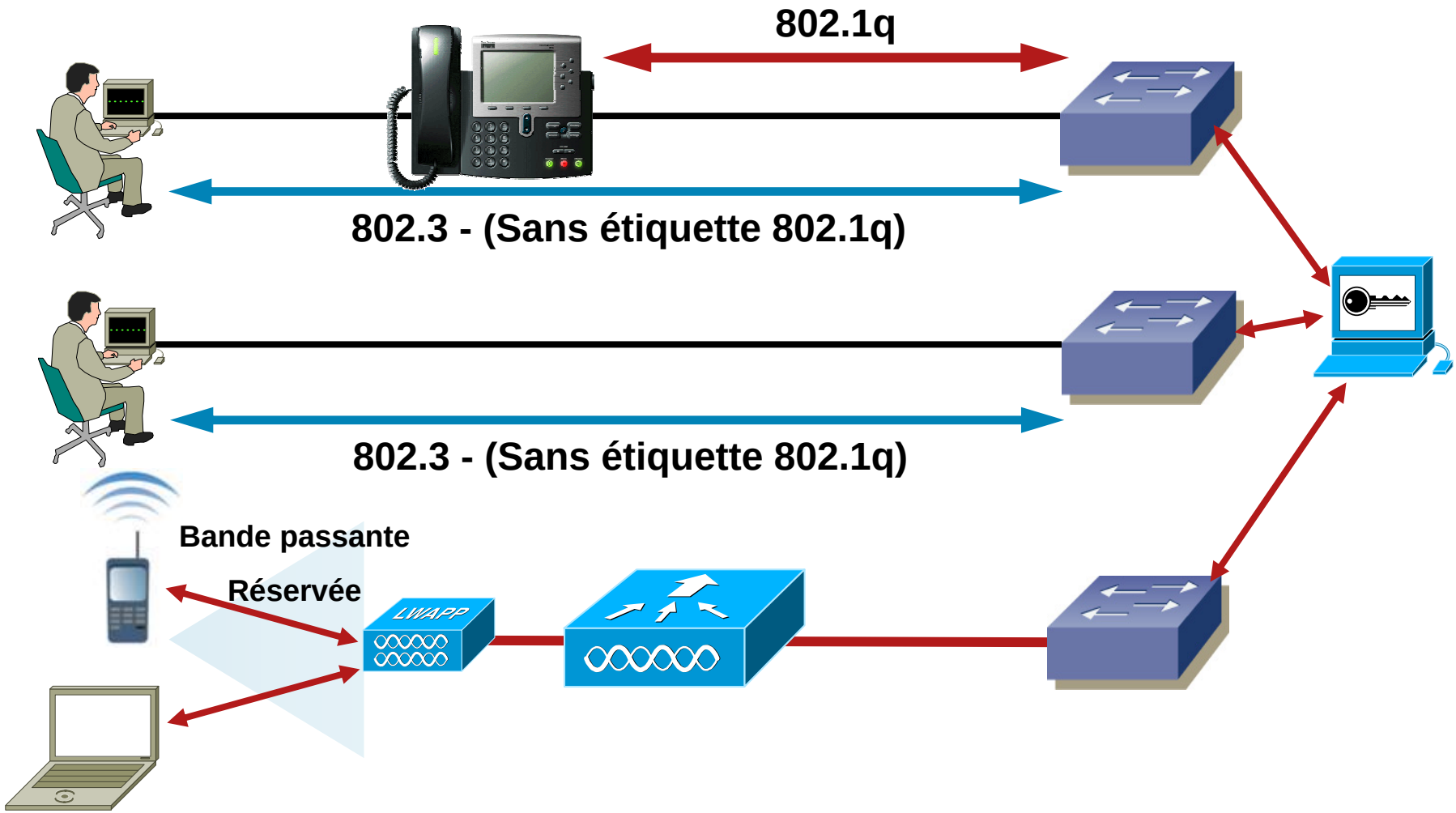
Prévenir la propagation de virus et des vers

Programme

- **Authentification**
  - **Qui peut accéder le réseau**
  - **L'impact de la téléphonie**
  - **802.1x, les visiteurs, Web Base Authentification**
- La conformité des postes au moment de la connexion
  - Sur le LAN, en VPN, etc...
- Les bonnes pratiques pour le contrôle des usagers connectés au réseau
  - Fonctions de sécurité présentent dans les commutateurs Cisco
  - QoS déployée?
  - Cisco Securité Agent (CSA)
- La surveillance et la configuration du réseau



Cisco Self Defending Network
Authentification et Autorisation



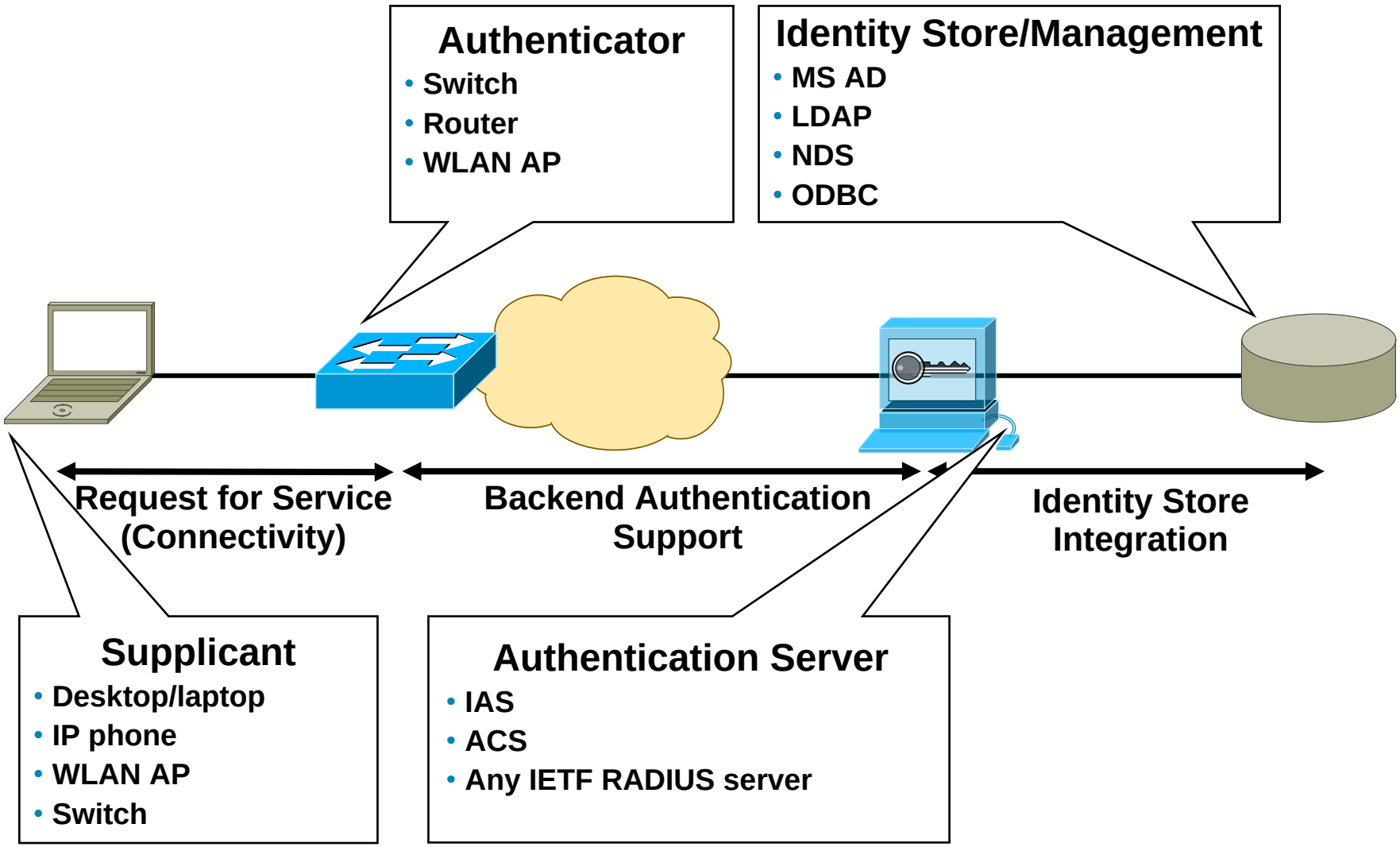
IEEE 802.1x - wired

- Standard set by the IEEE 802.1 working group
- Is a framework designed to address and provide port-based access control using authentication
- Primarily 802.1x is an encapsulation definition for EAP over IEEE 802 media—EAPOL (EAP over LAN) is the key protocol
- Layer 2 protocol for transporting authentication messages (EAP) between supplicant (user/PC) and authenticator (switch or access point)
- Assumes a secure connection
- Actual enforcement is via MAC-based filtering and port-state monitoring

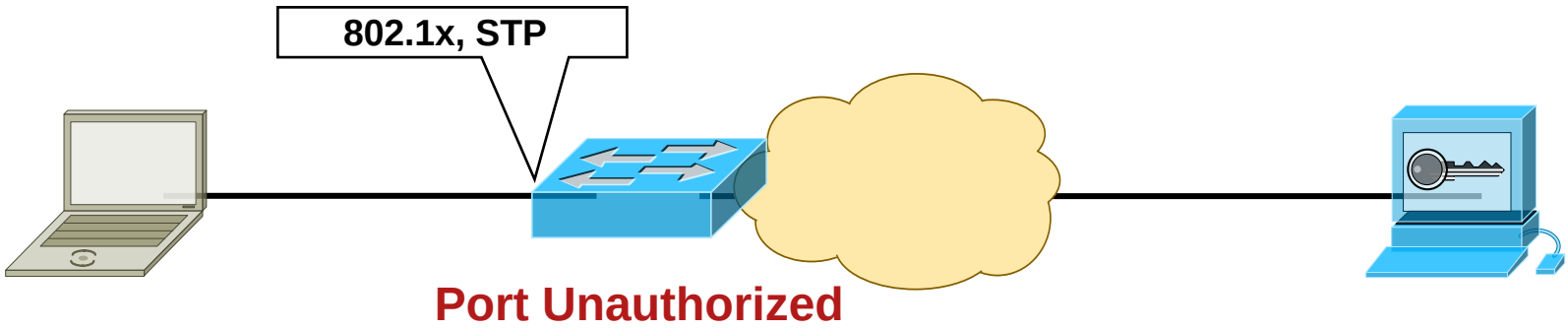
Some IEEE Terminology

IEEE Terms	Normal People Terms
Supplicant	Client
Authenticator	Network Access Device
Authentication Server	AAA/RADIUS Server

802.1x Port Access Control Model



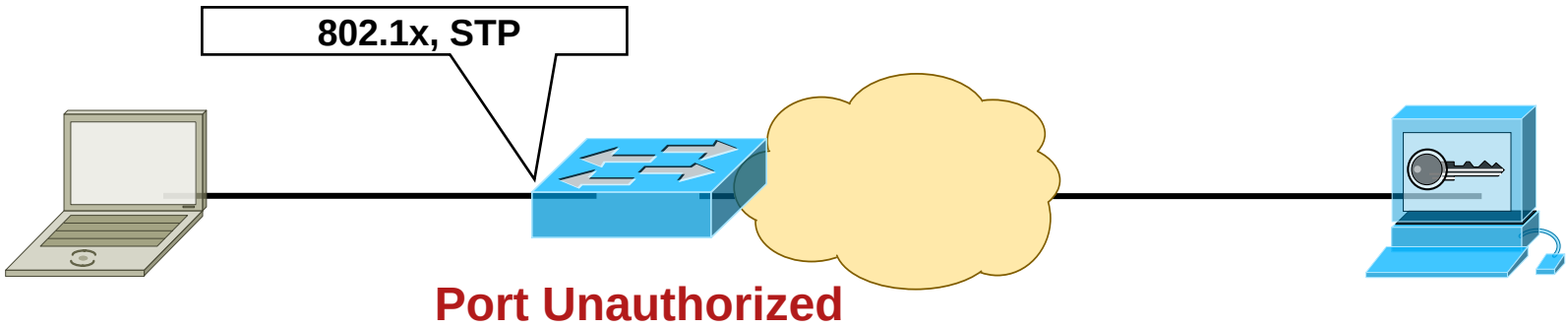
A Closer Look:



Cisco IOS

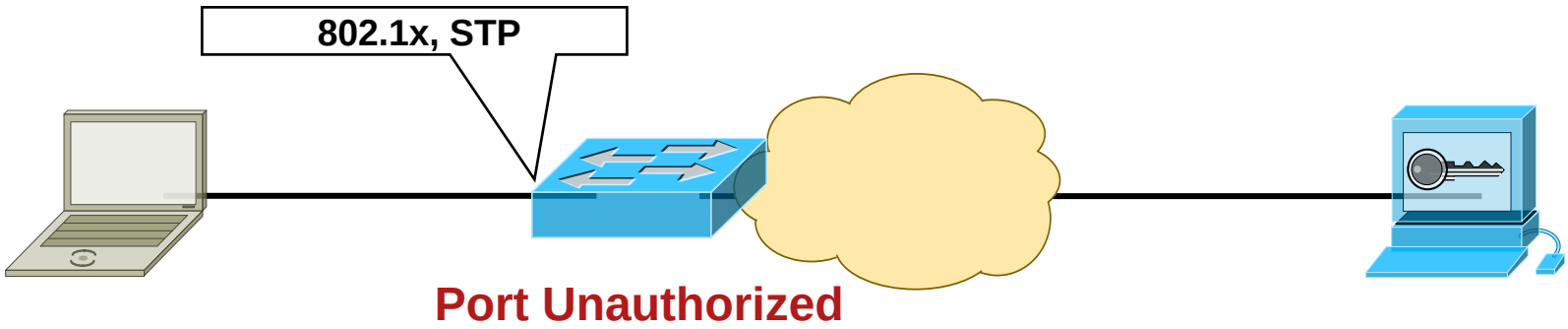
```
aaa authentication dot1x default group radius
aaa authorization network default group radius

radius-server host 10.100.100.100
radius-server key cisco123

dot1x system-auth-control

interface GigabitEthernet1/0/1
 dot1x port-control auto
```

A Closer Look:

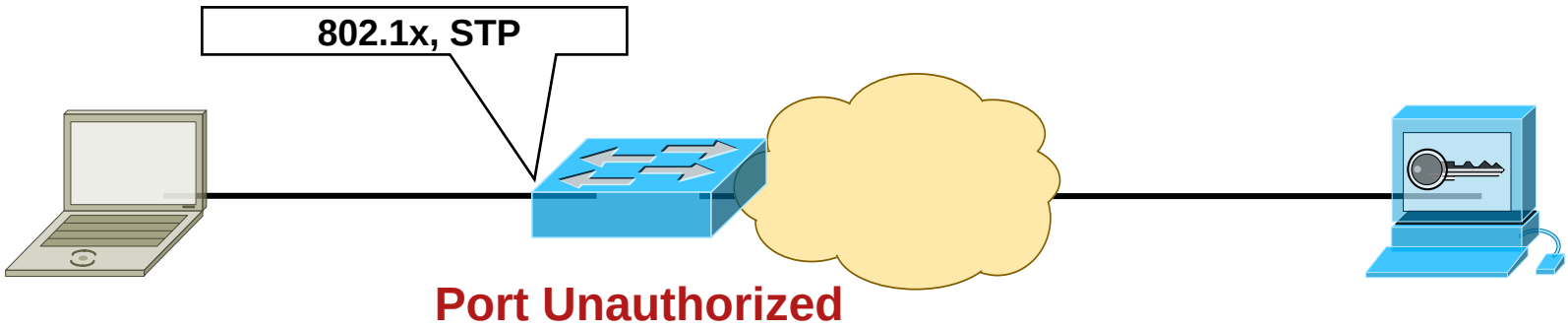


802.1x

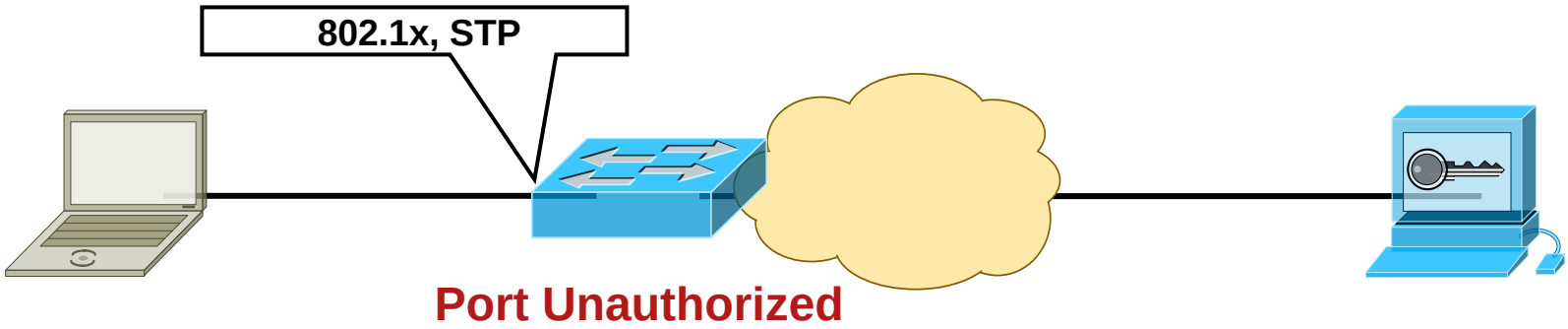
A Closer Look:



A Closer Look:



A Closer Look:



Port Unauthorized

EAPOL-Start

EAP-Identity-Request

EAP-Identity-Response

EAP—Method Dependent

EAP-Auth Exchange

Auth Exchange w/AAA Server

EAP-Success/Failure

Authentication Successful/Rejected

Port Authorized

Policy Instructions

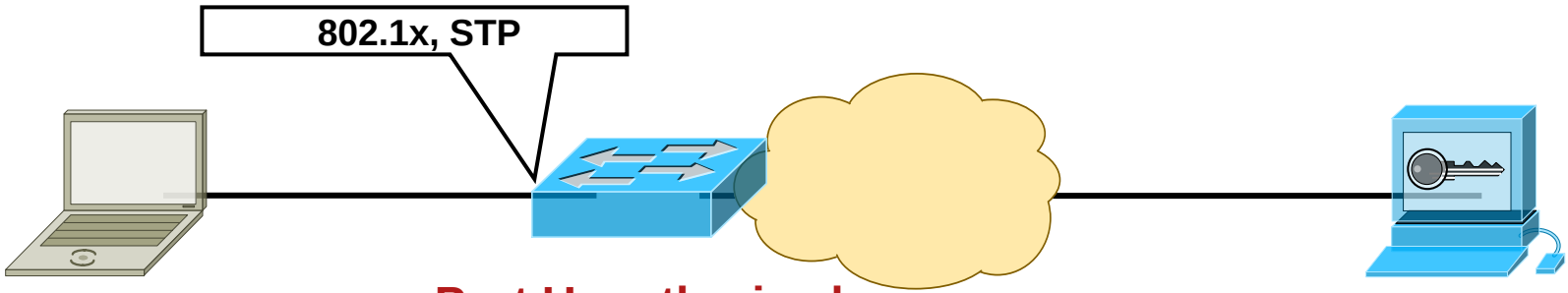
Port Unauthorized

EAPOL-Logoff

802.1x

RADIUS

A Closer Look:



Port Unauthorized

EAPOL-Start

EAP-Identity-Request

EAP-Identity-Response

EAP—Method Dependent

EAP-Auth Exchange

Auth Exchange w/AAA Server

EAP-Success/Failure

Authentication Successful/Rejected

Port Authorized

Policy Instructions

Port Unauthorized

EAPOL-Logoff

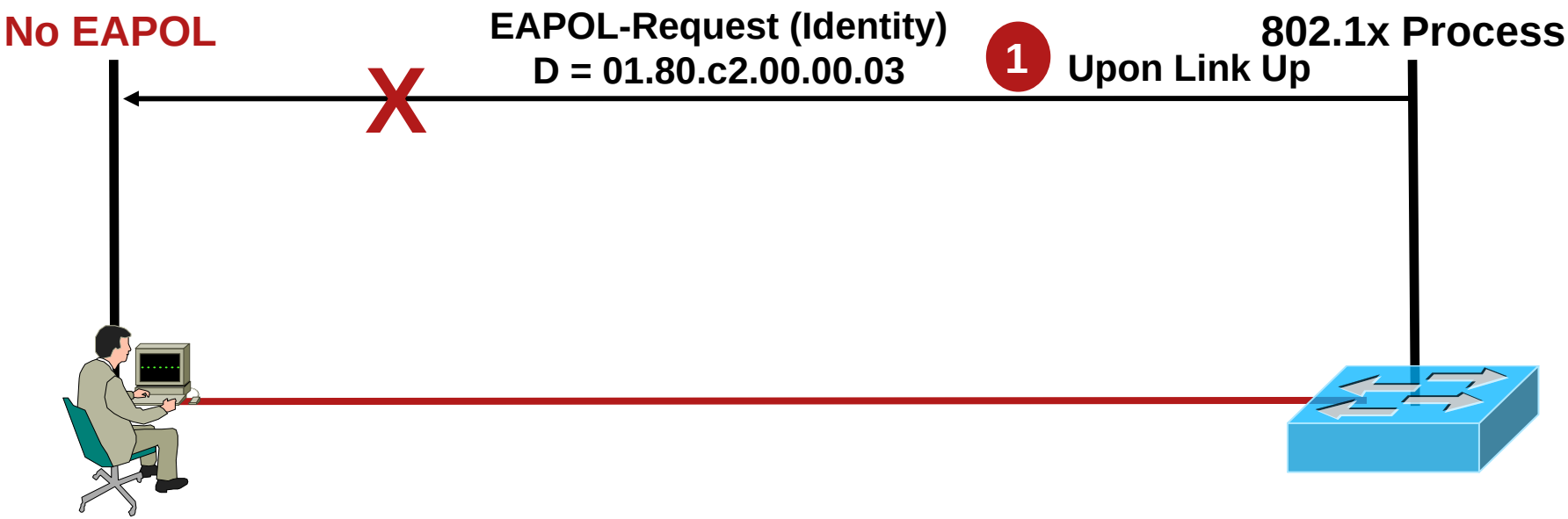
Actual Authentication Conversation Is Between Client and Auth Server Using EAP; the Switch Is an EAP Conduit, but Aware of What's Going on

802.1x

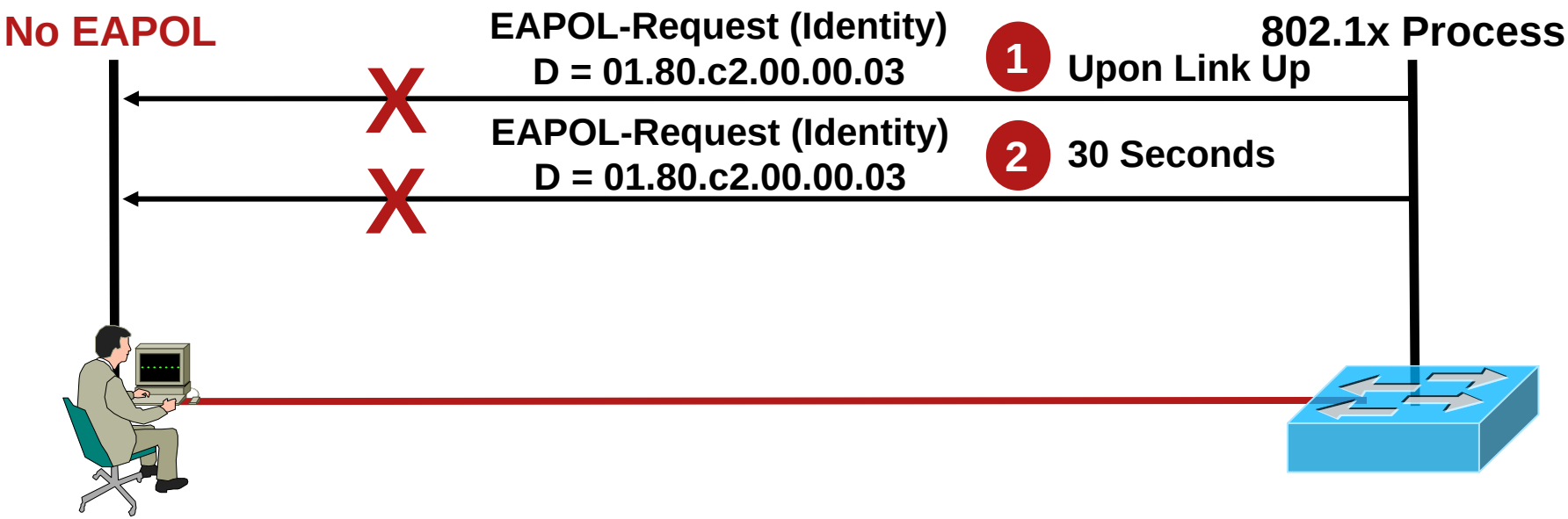
RADIUS

802.1x: Default Operation

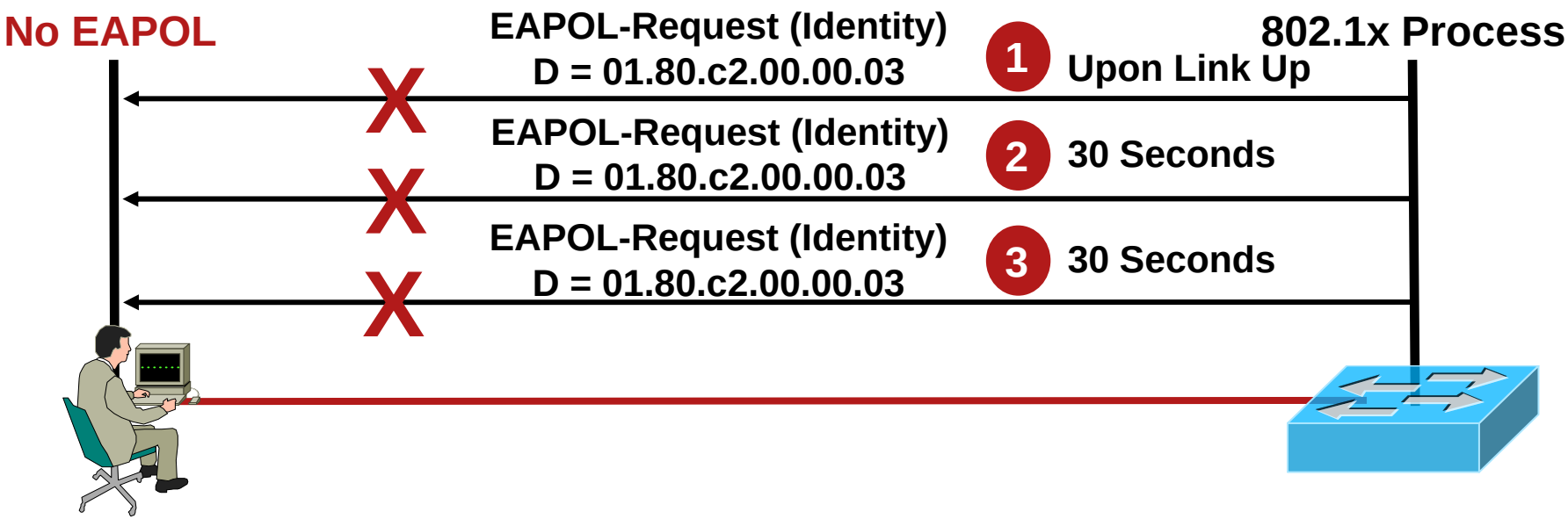
802.1x: Default Operation



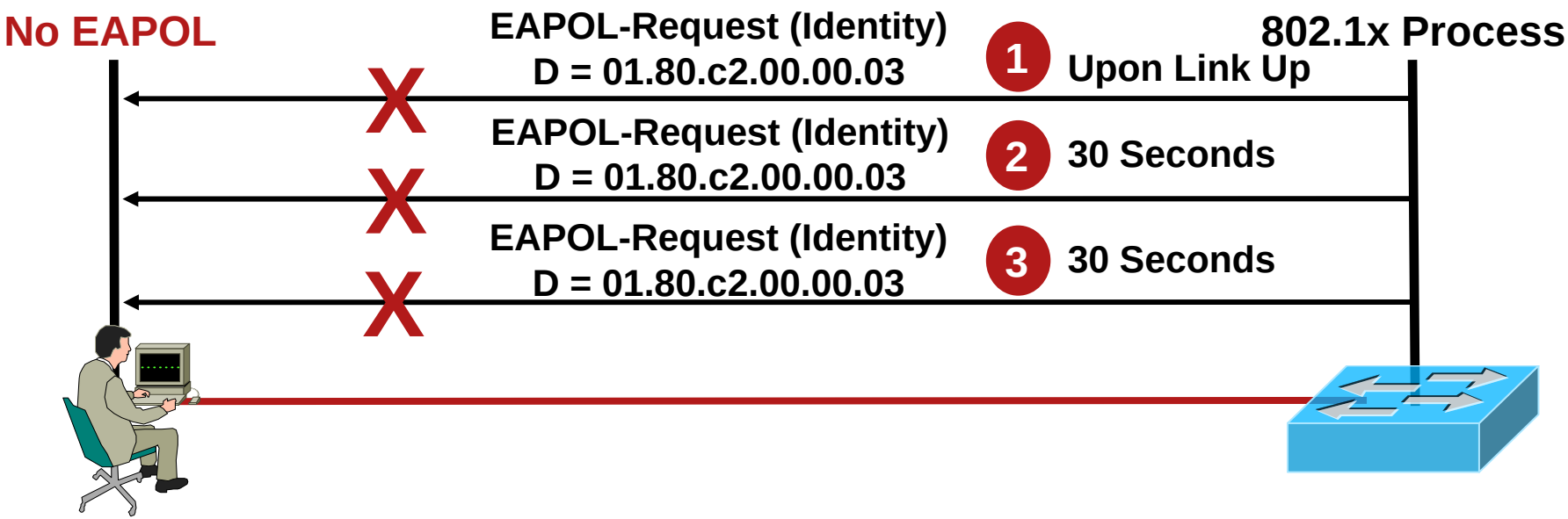
802.1x: Default Operation



802.1x: Default Operation



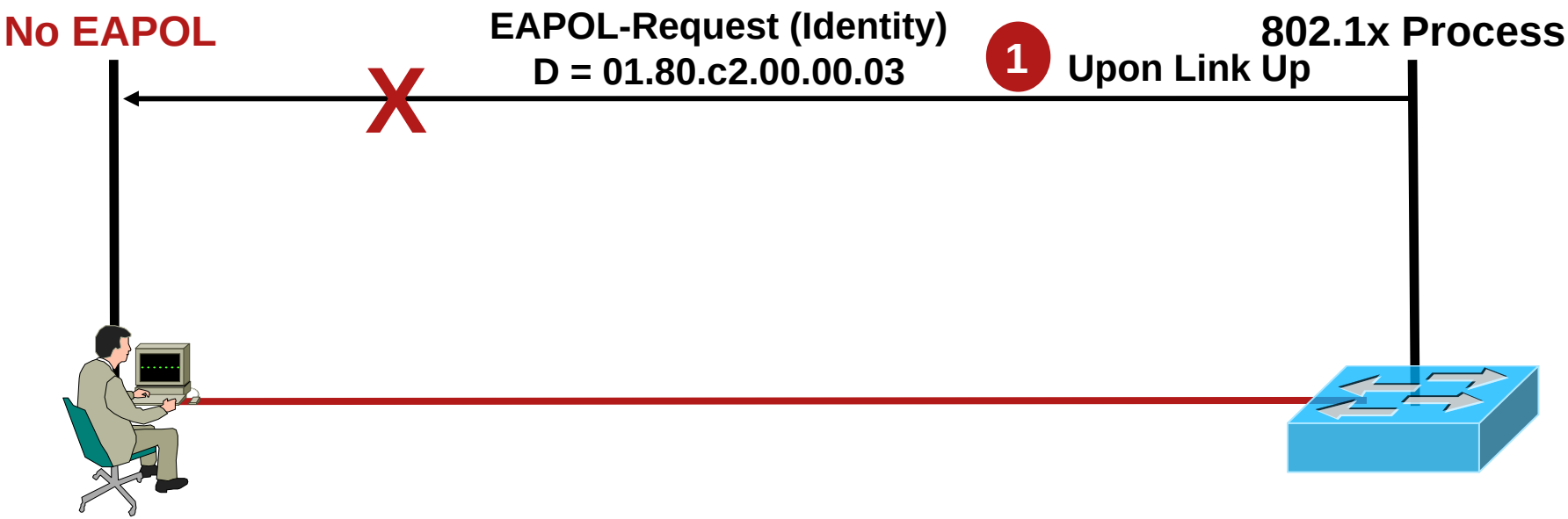
802.1x: Default Operation



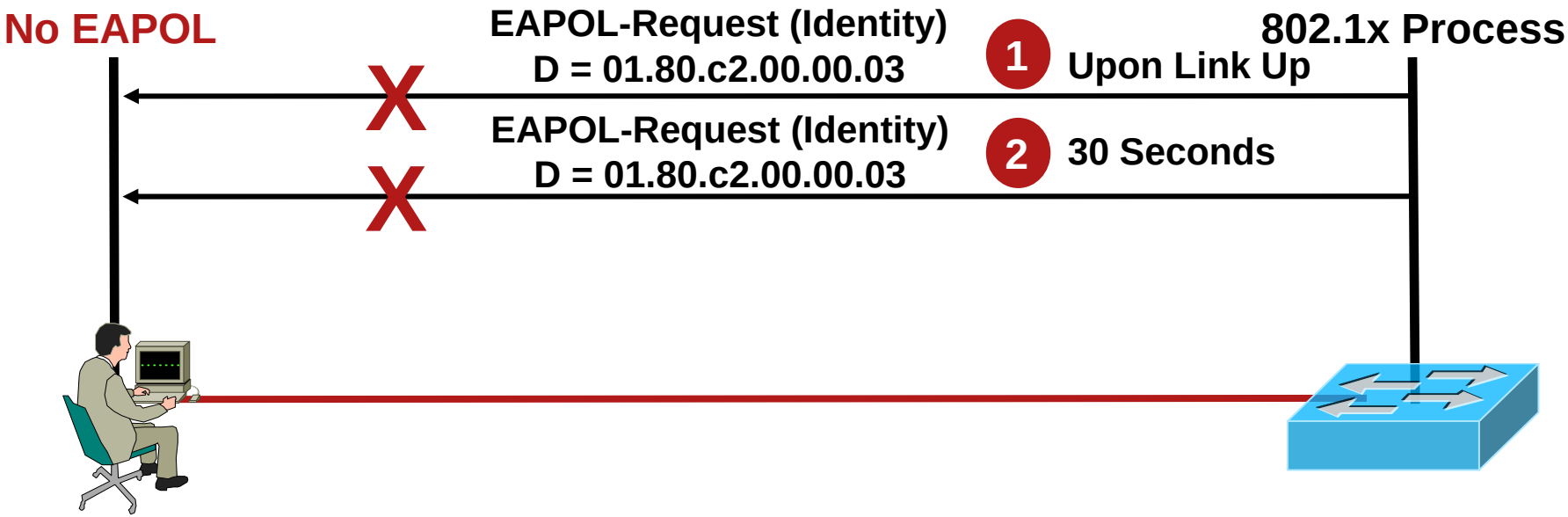
- Any 802.1x-enabled switch port will send EAPOL identity-request frames on the wire (whether a supplicant is there or not)
- Switch defaults to no supplicant being on the wire based on no EAPOL response to its requests
- No network access is given
- Transient state; whole process restarts after a hold timer
- Process can start again if a supplicant appears on the port

802.1x with Guest VLAN

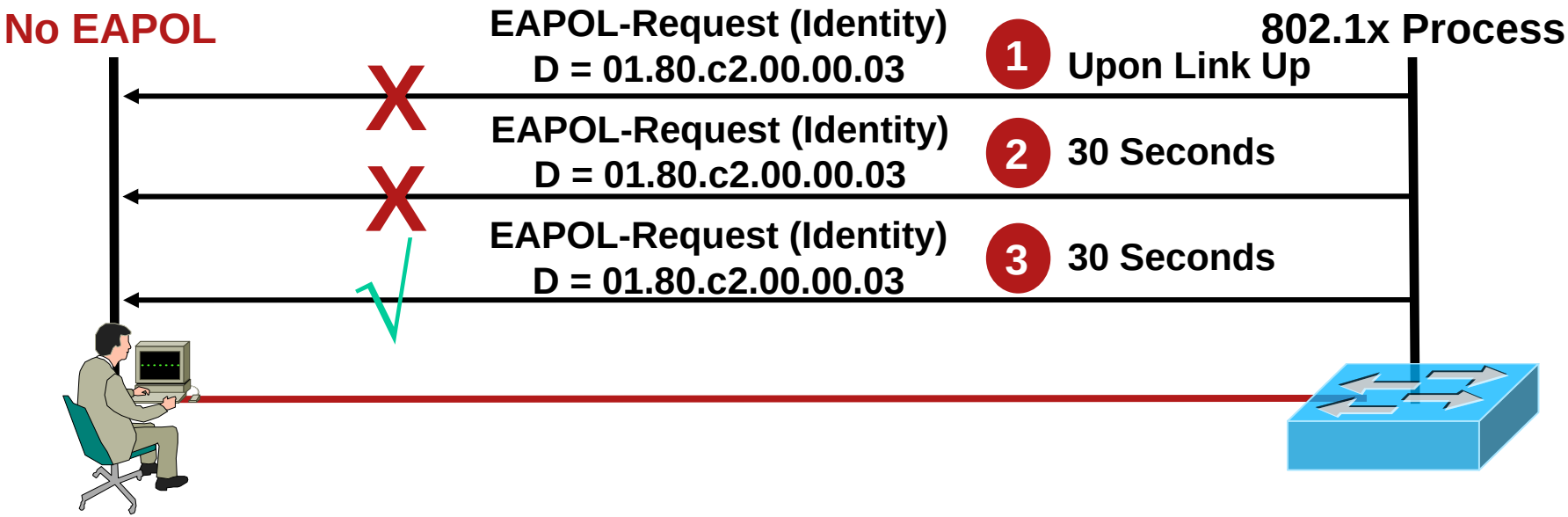
802.1x with Guest VLAN



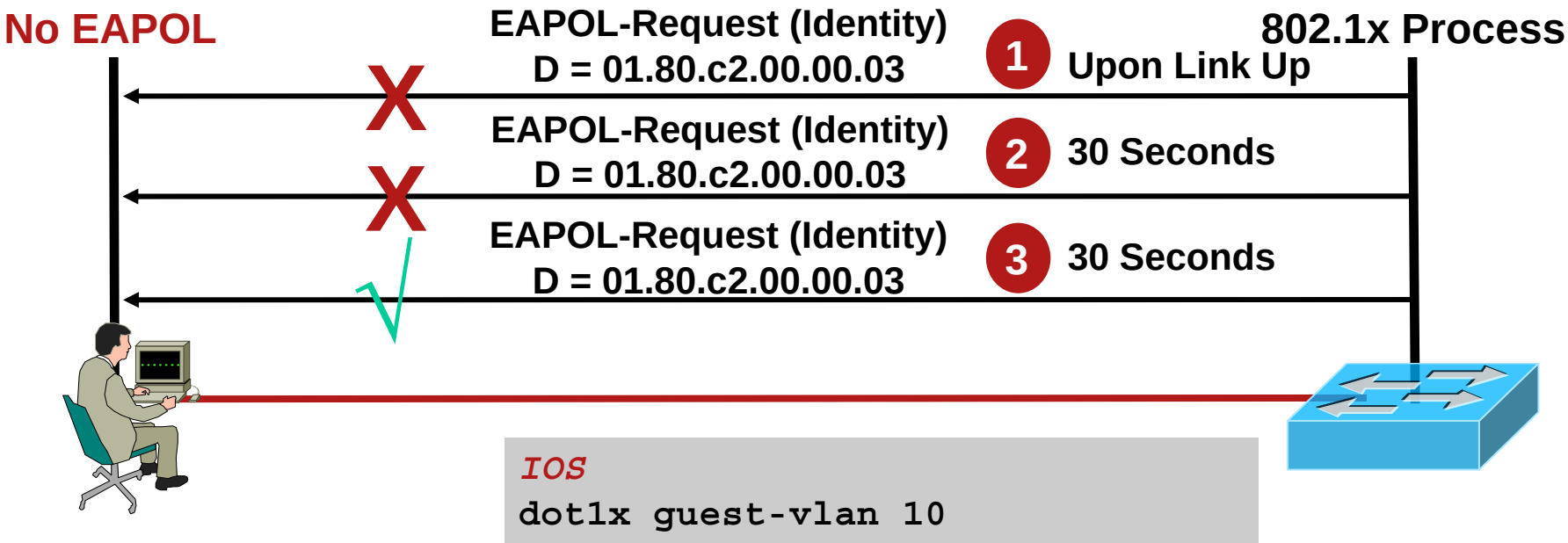
802.1x with Guest VLAN



802.1x with Guest VLAN



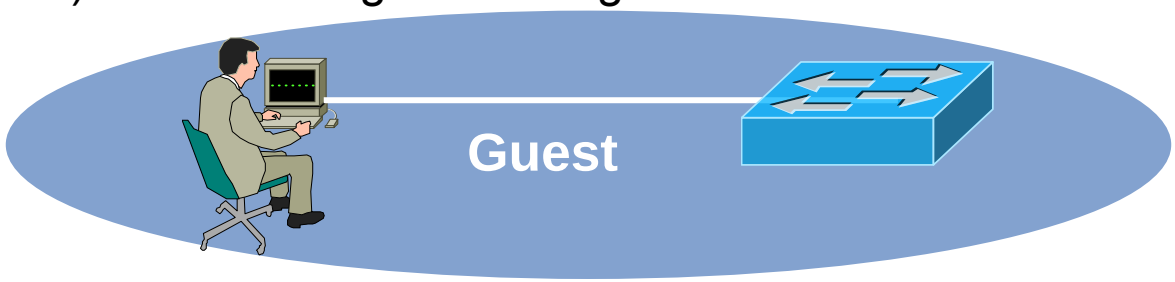
802.1x with Guest VLAN



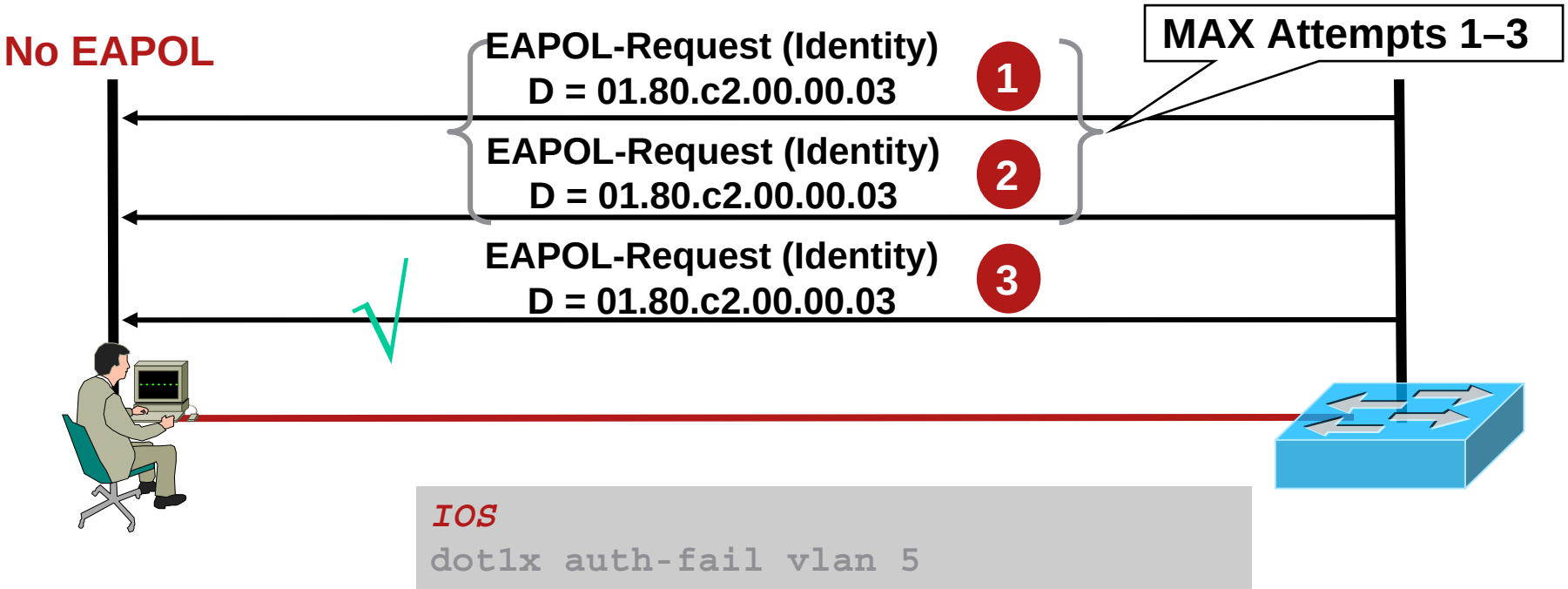
- Any 802.1x-enabled switch port will send EAPOL-Identity-Request frames on the wire (whether a supplicant is there or not)
- Port is moved to guest VLAN after step three above; instead of transitioning to disconnected, the port immediately transitions to a state of authorized and the auth-SM state is authenticated

802.1x with Guest VLAN

- Default timeout is 30 seconds with three retries; total timeout period is 90 secs by default
- A device is deployed to guest VLAN based on lack of response to switch's EAPOL-Identity-Request frames (which can be thought of as 802.1x hellos)
- No further security or authentication to be applied
- It is exactly like the administrator deconfigured 802.1x, and hard-set the port into a determined VLAN
- No machines that speak 802.1x (or who can indeed respond to the switch via EAPOL) should ever go into the guest VLAN



802.1x with Auth Fail VLAN

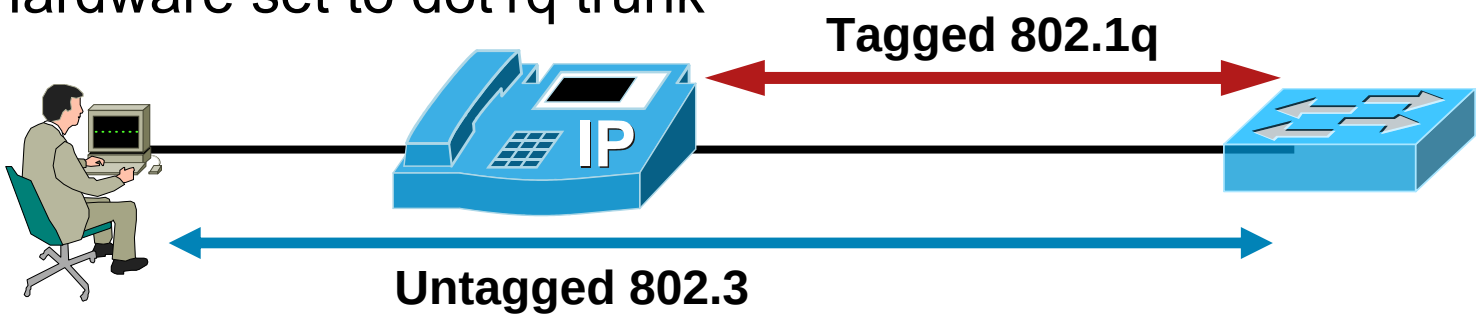


- Any 802.1x-enabled switch port will send EAPOL-Identity-Request frames on the wire (whether a supplicant is there or not)
- Port is moved to auth fail VLAN after step three above; instead of transitioning to disconnected, the port immediately transitions to a state of authorized and the auth-SM state is authenticated
- Requires correct supplicant behavior

- DEMO OF 802.1x

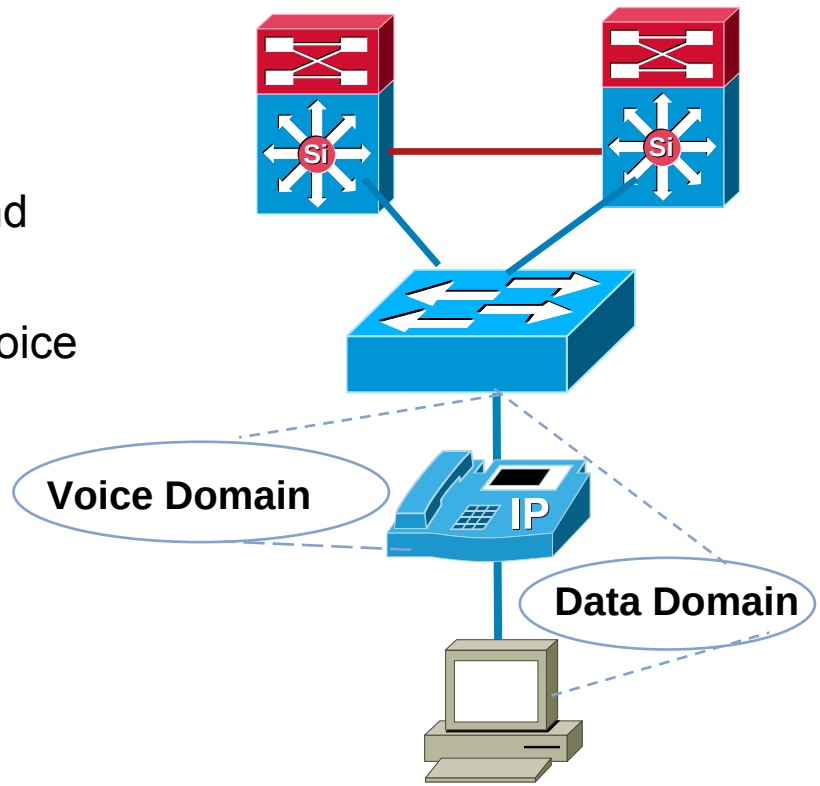
802.1x with VVID (Voice, Video and Integrated Data)

- **Multi Domain Authentication (MDA)**
- With Multi-VLAN Access Ports, a port can belong to two VLANs, while still allowing the separation of voice/data traffic while enabling you to configure 802.1x
- An access port able to handle two VLANs
  - Native or Port VLAN Identifier (PVID)
  - Auxiliary or Voice VLAN Identifier (VVID)
- Hardware set to dot1q trunk



Multi Domain Authentication (MDA)

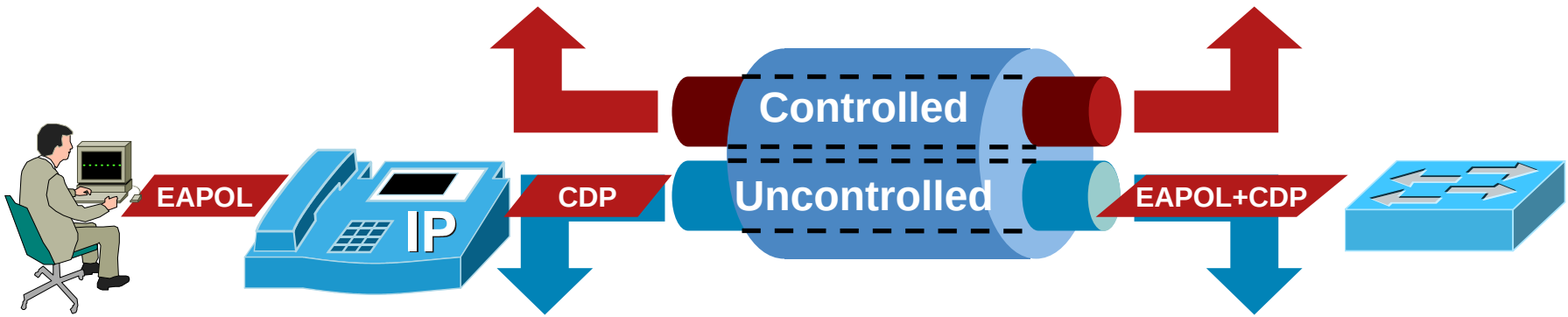
- **Deployment : IP phone (Cisco or 3rd party) + single host behind the phone**
- Enhanced security with independent 802.1x authentication and authorization of IP phone and host
- Host is placed in data VLAN, and IP phone in voice VLAN - on the same switch port
- Data VLAN can be downloaded from RADIUS server



802.1x with VVID

For Each 802.1x Switch Port, the Switch Creates Two Virtual Access Points at Each Port

The Controlled Port Is Open Only When the Device Connected to the Port Has Been Authorized by 802.1x



Uncontrolled Port Provides a Path for Extensible Authentication Protocol over LAN (EAPOL) and CDP Traffic only

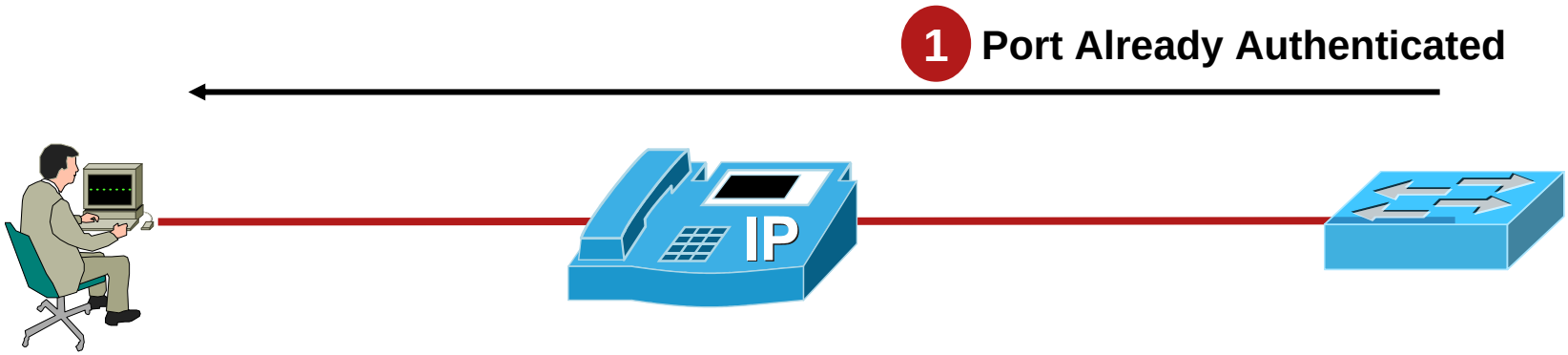
802.1x with VVID

- A dot1x-vvid port is an MDA, that has dot1x configured
- The PC has to authenticate before getting access to the data VLAN
- The IP phone (without dot1x supplicant implementation) can get access to the voice VLAN after sending proper CDP packets, regardless of the dot1x state of the port


```
IOS
switchport mode access
switchport access vlan 2
switchport voice vlan 12
dot1x port-control auto
```

- Unauthenticated voice VLAN (VVID) access
- Authenticated data VLAN (PVID) access
- This allows 802.1x and VoIP to coexist at the same time

802.1x with VVID: Previous Limitations



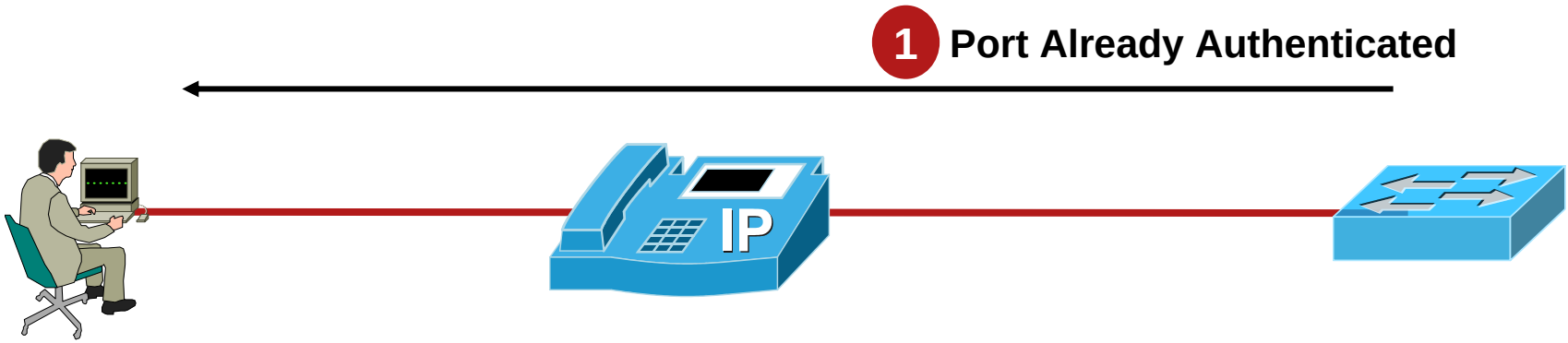
802.1x with VVID: Previous Limitations

If an End-User Disconnects, the Port Remains Authorized by 802.1x

802.1x with VVID: Previous Limitations

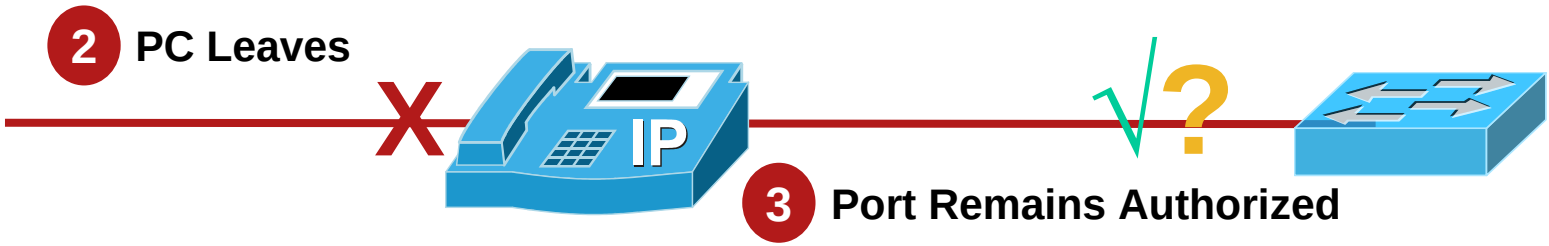
- An illegitimate user can now gain access to the port by spoofing the authenticated MAC address, and bypass 802.1x completely—security hole
- In an attempt to workaround this, some customers have enabled periodic reauthentication of end-devices
- This is not the reason to enable reauthentication
- We need to deal with the fact that any machine can disappear from the network and the switch (and 802.1x) does not know about it explicitly (i.e. link doesn't go down)

802.1x with VVID: Previous Limitations



802.1x with VVID: Previous Limitations

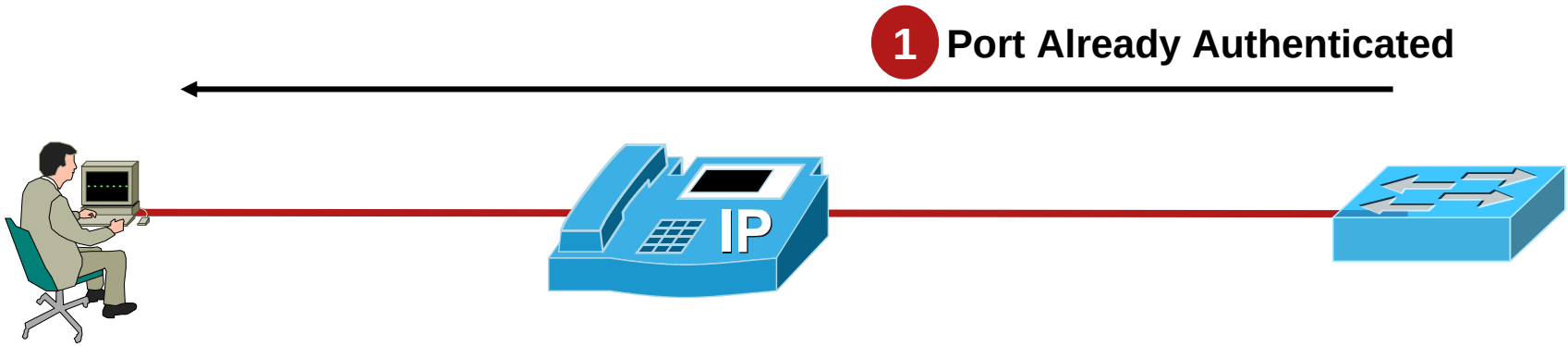
If an End User Disconnects, the Port Remains Authorized by 802.1x



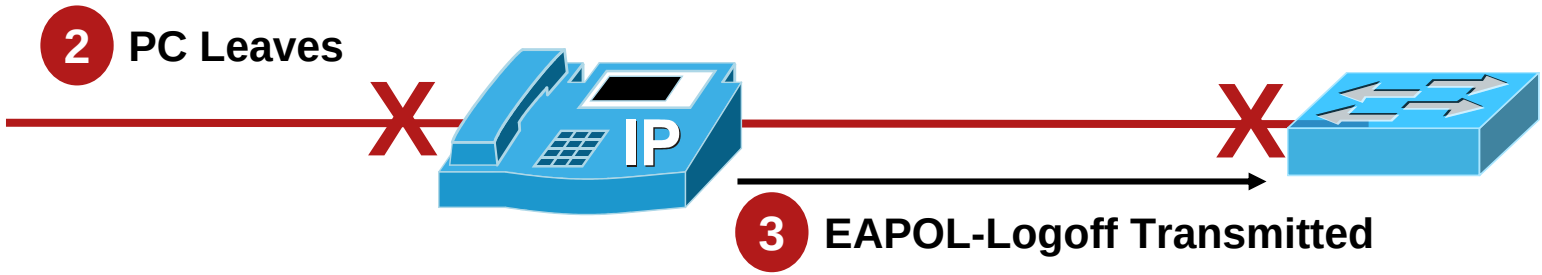
802.1x with VVID: Previous Limitations

- A legitimate user may now attempt to gain access to the port by way of 802.1x
- However, assuming MAC addresses are different, now the switch may treat this as a security violation
- In an attempt to workaround this, some customers have enabled periodic reauthentication of end-devices
- This is not the reason to enable reauthentication
- Overall, same issue as previous slides

802.1x with VVID: EAPOL-Logoff



802.1x with VVID: EAPOL-Logoff



- If an end-user disconnects, an IP phone transmits an EAPOL-logoff frame to the switch

  SA = PC MAC address

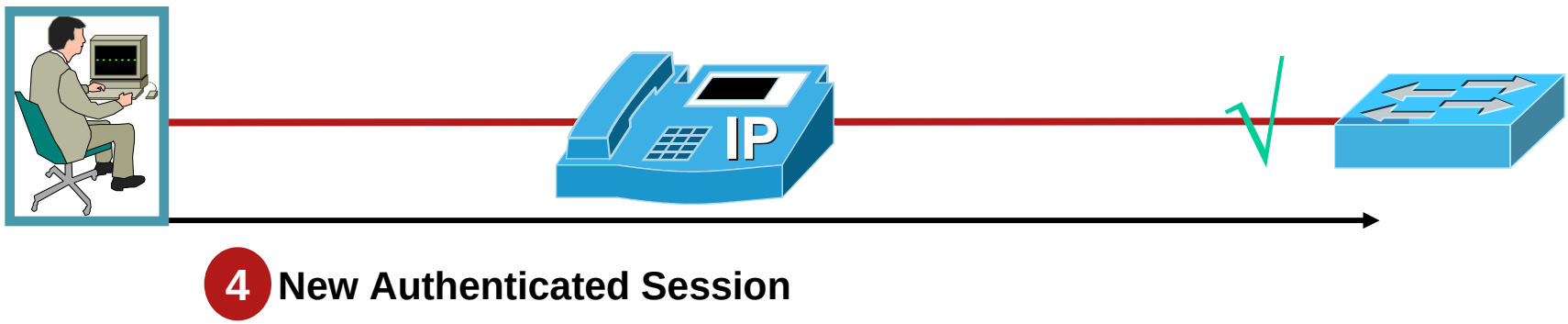
  DA = 01-80-C2-00-00-03 (PAE group address)

- Two basic functions needed from phone

  Monitor the **PAE** group address to determine who and where supplicant is

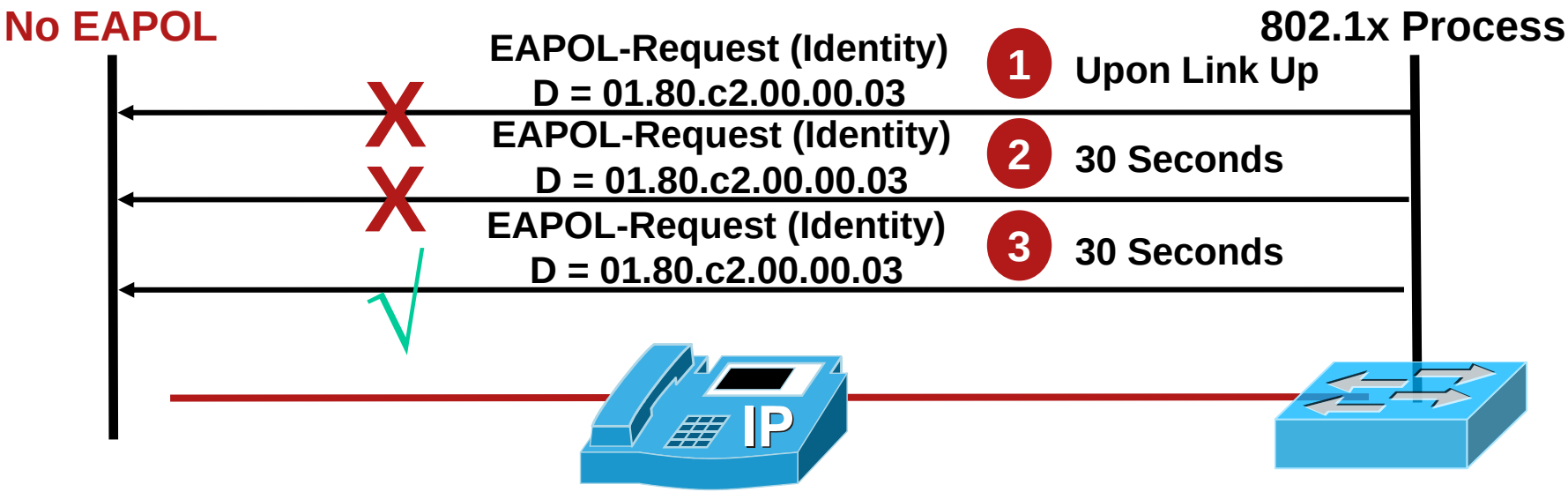
  Actually transmitting the EAPOL-logoff frame

802.1x with VVID: EAPOL-Logoff



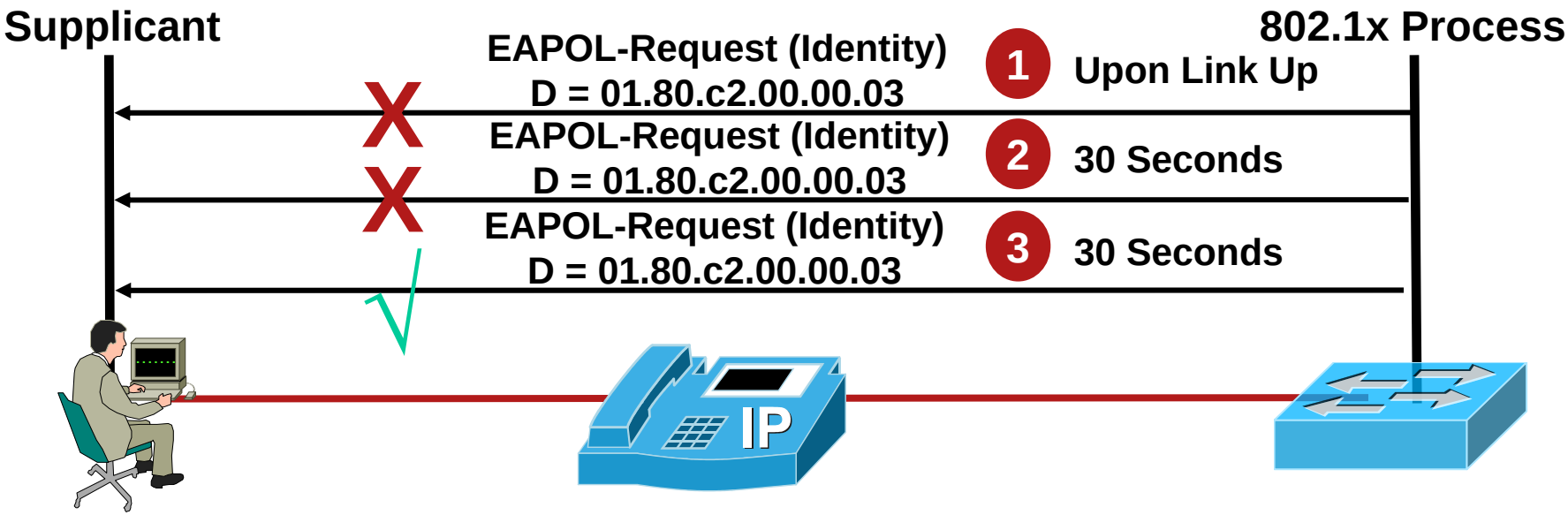
- The switch thinks it is a standard EAPOL-logoff frame transmitted by a supplicant indicating end of service
- This closes the current security hole, and promotes subsequent mobility

802.1x with VVID: Deployment Issues



- Assuming no supplicant on the wire, a port will be deployed into the guest VLAN after step three above, if guest VLAN is configured

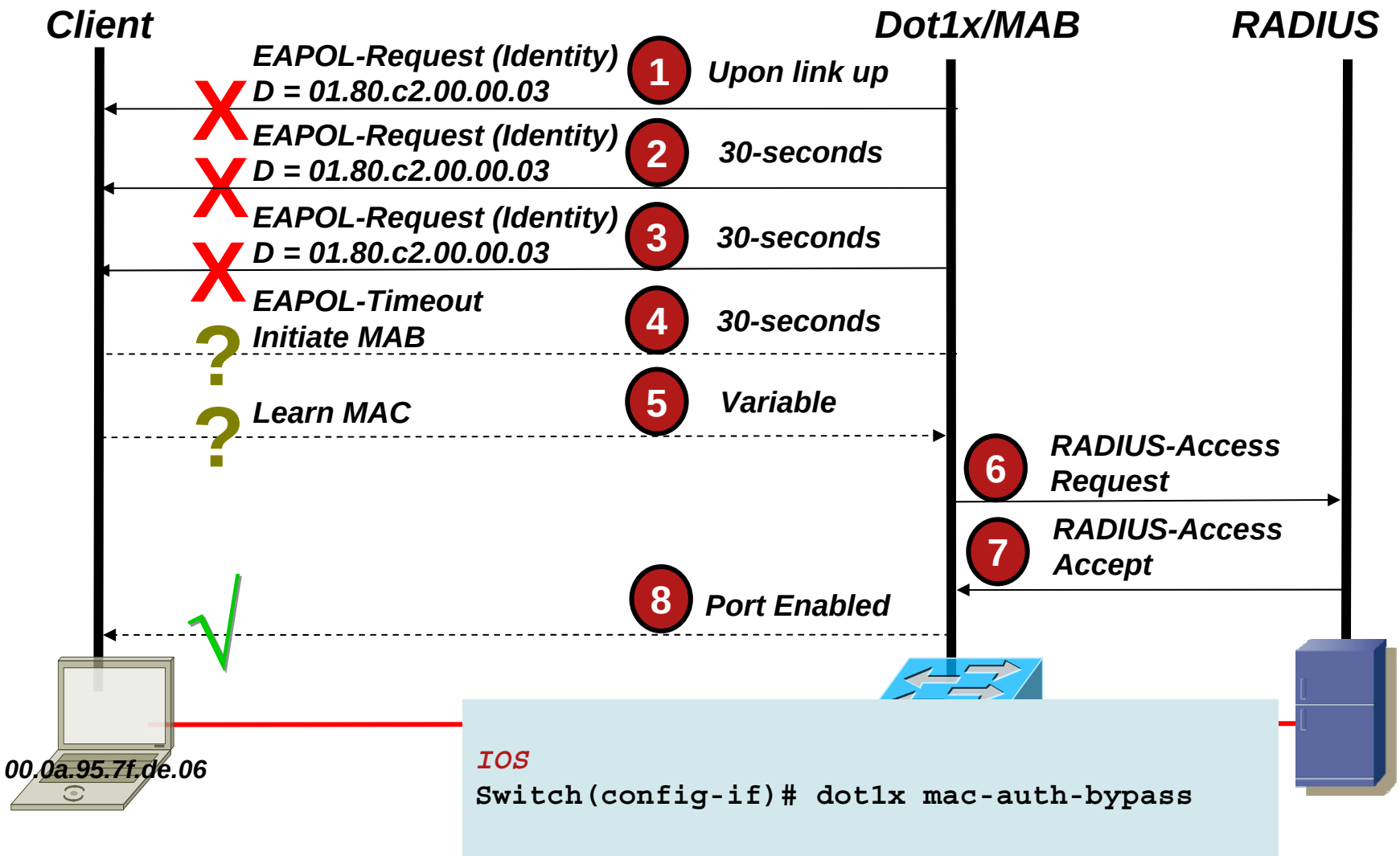
802.1x with VVID: Deployment Issues



- If any user plugs into a phone, 802.1x is now totally dependent on how their supplicant is configured to operate
- By default, Microsoft Windows supplicants do not send EAPOL-starts; you will want to know why 802.1x works when you plug into a switch, and why it doesn't work when you plug into a phone

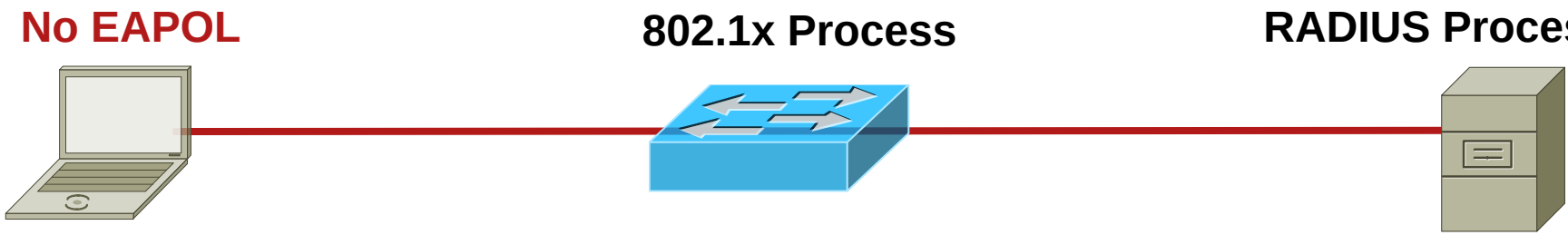
- DEMO OF MDA

MAC Authentication Bypass (MAB)



- DEMO OF MAB ?

Web Based Proxy Authentication

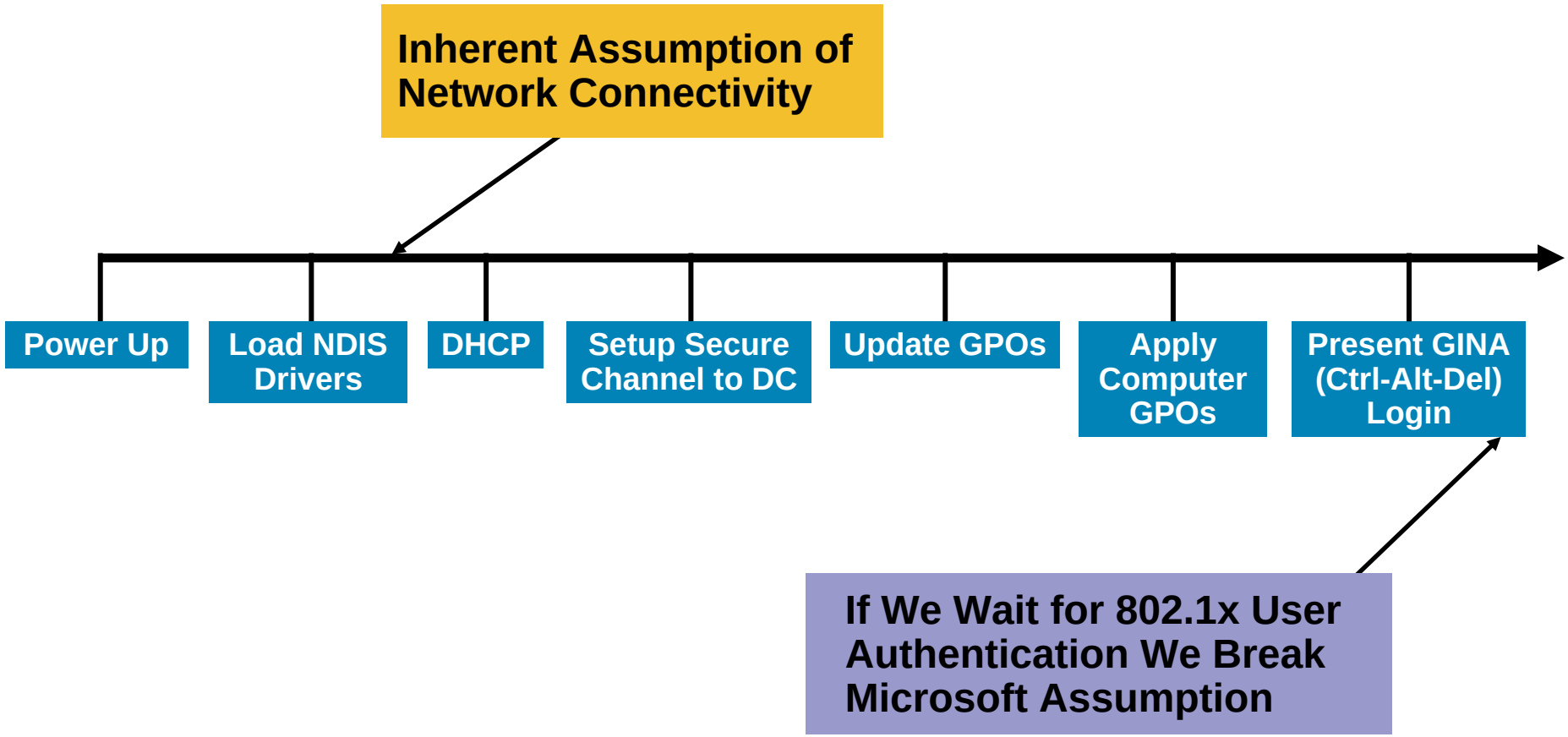


1. 802.1x Timeouts
2. Client Initiates Connection—Activates Port Authentication State Machine
3. Switch Port Filters Traffic Limiting It to HTTP, HTTPS, DNS and DHCP
4. Switch Port Relays DHCP Address from DHCP Server
5. User Starts Web Browser and Initiates Web Connection
6. Switch Port Redirects URL and Presents HTTP Form Prompting for Userid/Pwd
7. User Enters Credentials—They Are Checked Against RADIUS DB—If Authenticated Then Switch Port Opened for Normal Network Access

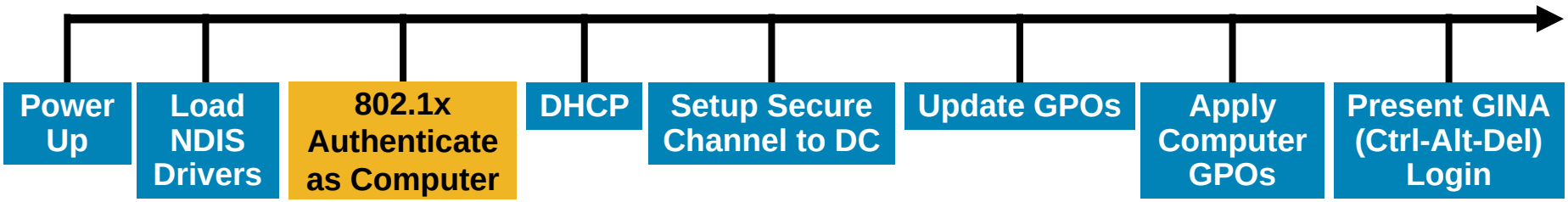
- DEMO of Web based auth

Operating System Implementations

Windows Boot Cycle Overview



Windows Boot Cycle Overview



Microsoft and Machine Authentication

- What is machine authentication?

  The ability of a Windows workstation to authenticate under its own identity, independent of the requirement for an interactive user session

- What is it used for?

  Machine authentication is used at boot time by Windows OSes to authenticate and communicate with Windows domain controllers in order to pull down machine group policies

- Why do we care?

  Pre-802.1x this worked under the assumption that network connectivity was a given; post-802.1x the blocking of network access prior to 802.1x authentication breaks the machine-based group policy model—UNLESS the machine can authenticate using its own identity in 802.1x

Windows Login Procedure

User Authentication

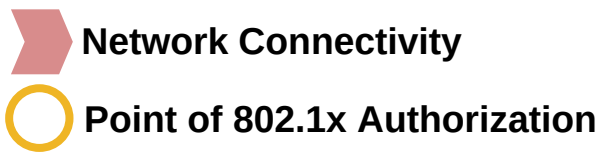
*** No Connectivity to Domain Controller Until User Logs In**

Machine Authentication

*** 802.1x Early in Boot Process**

Machine + user Authentication

*** Users Can Be Individually Authenticated**



Different Modes of Authentication in Microsoft Environments

- Controlled by registry keys
- Authentication by machine only

  No need for user authentication if machine authentication is successful

- Authentication by user only

  No machine authentication taking place at all—be careful, this breaks group and system policies

- Authentication by user and machine

  Uses authentication of both user and machine; switches contexts when going from one to the other

How Do You Enable Machine Auth?

- Make sure the computer is a member of the domain
- If using TLS, make sure the computer gets a cert—either through auto-enrollment or manually
- If using EAP-FAST, PEAP or EAP-TLS make sure that the CA cert is in the local machine store; typically added if CA is up when machine is added to the domain; if not, you can force via auto-enrollment too
- Click the check box for the “authenticate as computer when computer information is available” in the authentication tab of the local-area connection properties window

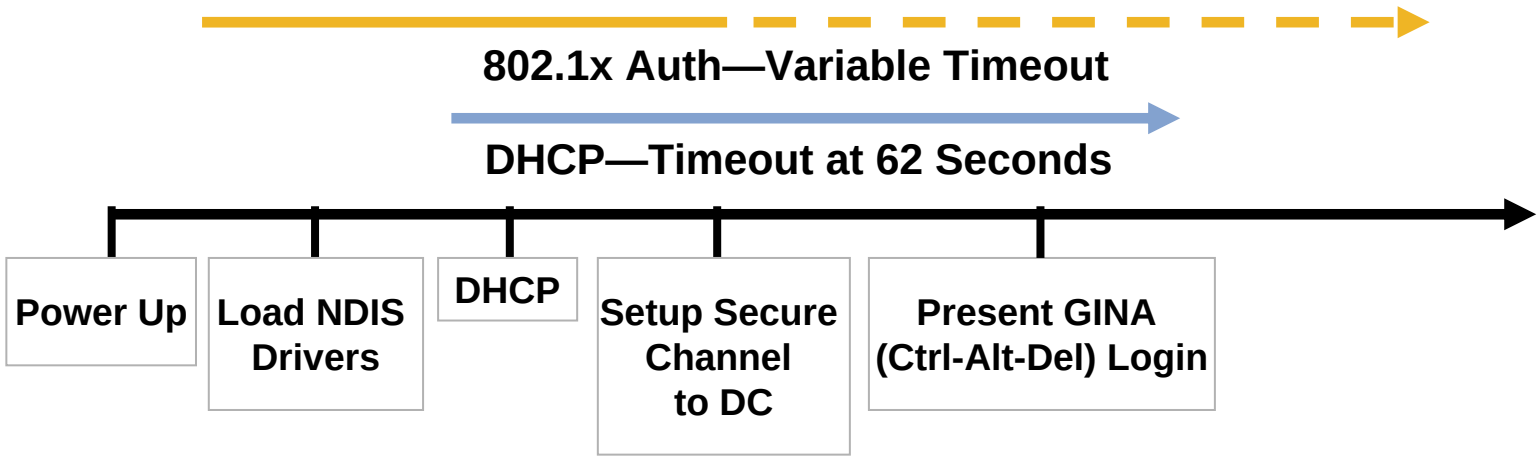
Machine Auth Using PEAP or TLS

- Machine authentication using PEAP
  - Uses account information for the computer created at the time the machine is added to the domain
  - Computer must be a member of the domain
  - If doing mutual authentication, the computer must trust the signing CA of the RADIUS server's cert
- Machine authentication using EAP-TLS
  - Authenticates the computer using certs
  - The computer must have a valid cert
  - If doing mutual authentication, the computer must trust the signing CA of the RADIUS server's cert
  - Easiest way to deploy is using MS-CA and Windows GPOs

Microsoft Issues with DHCP

DHCP Is a Parallel Event, Independent of 802.1x Authentication

- With wired interfaces a successful 802.1x authentication does not force a DHCP address discovery (no media-connect signal)
- This produces a problem if not properly planned
- DHCP starts once interface comes up
- If 802.1x authentication takes too long, DHCP may time out

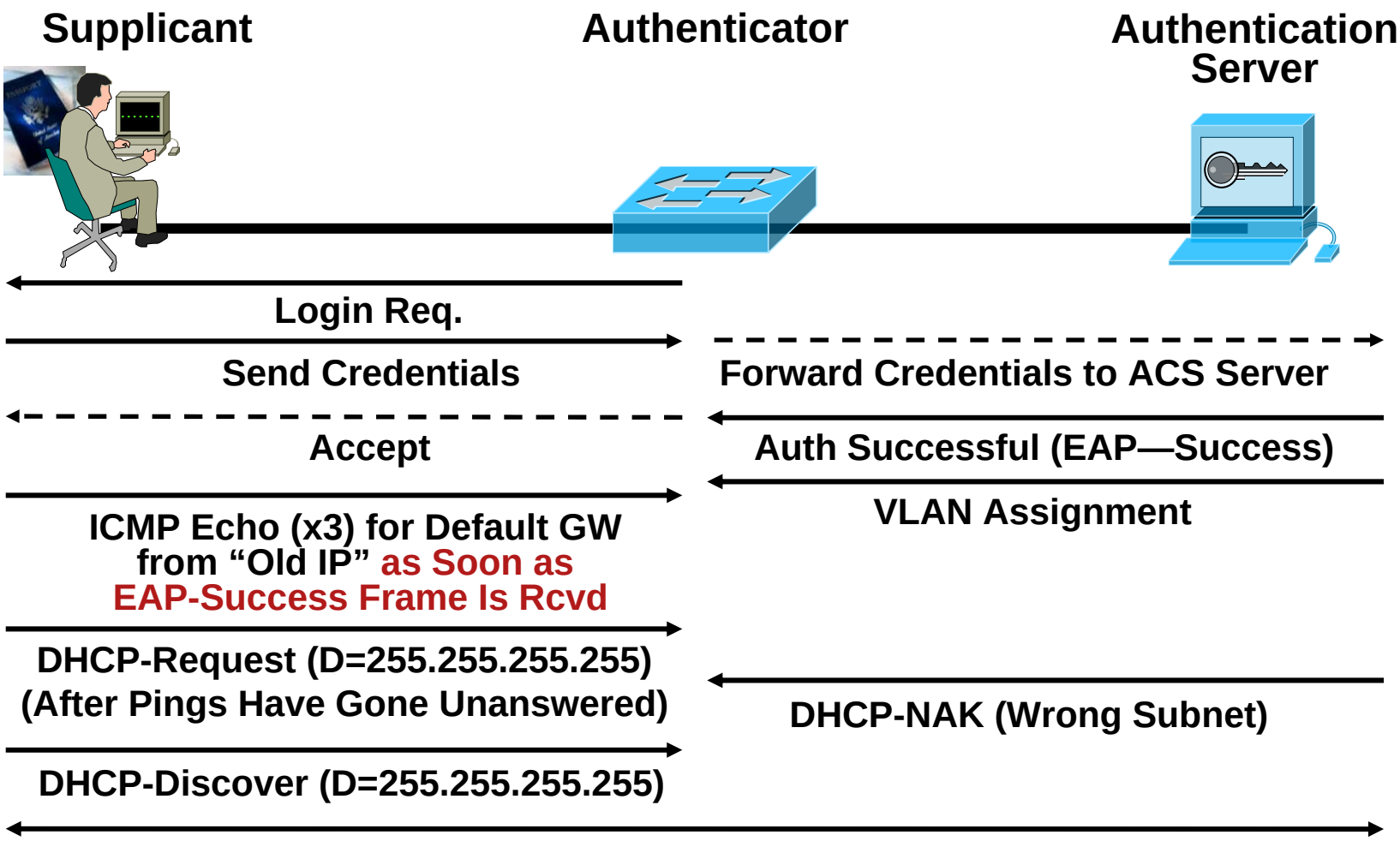


How to Address DHCP Timeout with 802.1x?

- Use machine authentication—this allows the initial machine authentication to obtain an IP address
- Supplicant behavior has been addressed by Microsoft
  - Windows XP: install service pack 1a + KB 826942
  - Windows 2000: install service pack 4
- Updated supplicants trigger DHCP IP address renewal
  - Successful authentication causes client to ping default gateway (three times) with a subsecond timeout
  - Lack of echo reply will trigger a DHCP IP renew
  - Successful echo reply will leave IP as is
  - Prerenewal ping prevents lost connections when subnet stays the same but client may be WLAN roaming

Microsoft Fixes

Windows XP: Install Service Pack 1a + KB 826942
Windows 2000: Install Service Pack 4



802.1x and Machine Access Restriction

Machine Authentication

- Machine boots up
- Interface becomes active (not authenticated)
- 802.1x authentication starts
- Machine sends its credential
  - EAP-TLS „Machine Certificate“
  - PEAP-MS-Chapv2 „Windows AD shared secret
  - EAP-FAST with CTA 2.0 supplicant machine authentication name prefix „host/“

User Authentication

- **If user logs on to machine, machine sends EAPOL-start message to notify the access point or switch that a new authentication is being performed**
- **Following EAP-TLS, PEAP-MS-Chapv2, EAP-FAST authentication will be done with users credential**

Note: Those Are Two Independent Authentications

802.1x and Machine Access Restriction

- If machine authentication fails or is not enabled, a user can still successfully access the network
- So machine authentication does not prevent users from accessing the network with a unregistered machine

User Authentication

- **If user logs on to machine, machine sends EAPOL-log-off message to notify the access point or switch that previous authentication is no longer valid anymore**
- **Following EAP-TLS, PEAP-MS-Chapv2, EAP-FAST authentication will be done with users credential**
- **Host/name format of the authentication request triggers MAR check**

802.1x and Machine Access Restriction

- User authentication is only successful after a previous successful machine authentication
- EAP-FAST, PEAP with EAP-MS-CHAPv2 and EAP-TLS only
- Allows to use machine authentication as a condition for user authorization
- This provides a way to deny authentication for a user because machine authentication to the network was not completed prior to a login attempt
- Machine authentication by itself does not prevent users from accessing the network with an unregistered machine; to enforce this restriction, ACS now only completes a user authentication if the MAC address associated with the attempt was previously included in a successful machine authentication

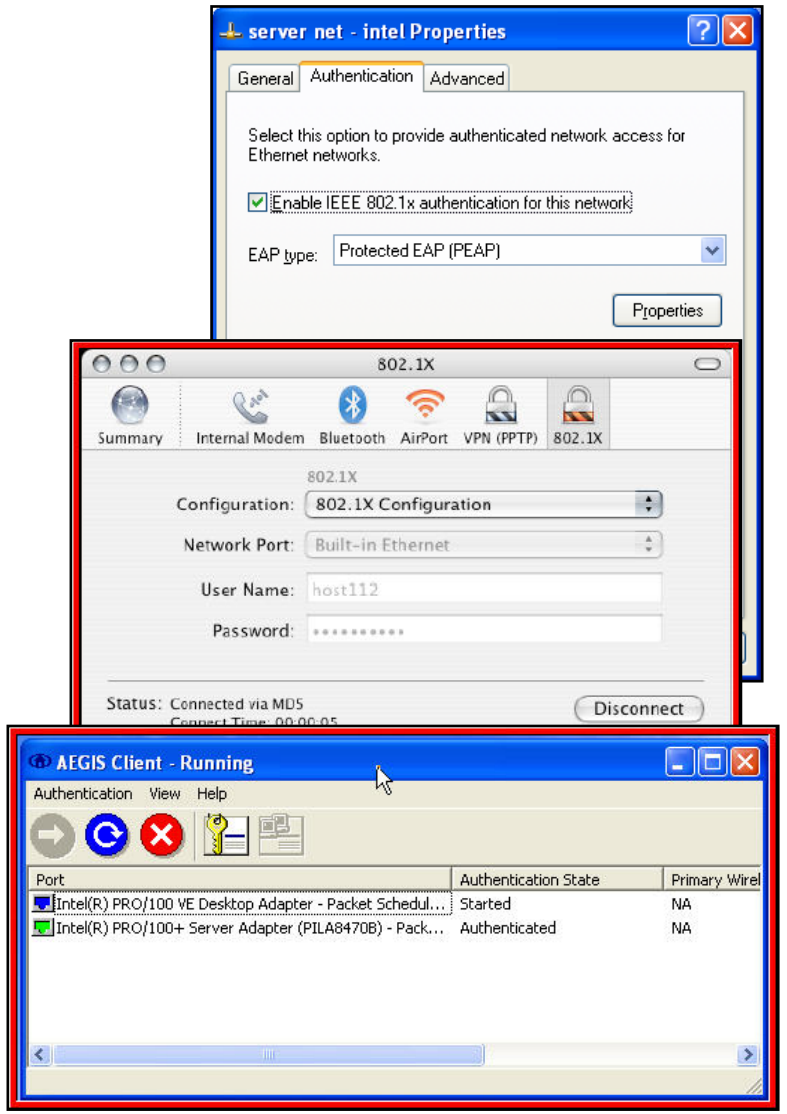
- DEMO Machine auth

802.1x Supplicant Support

- 802.1x requires client side code (supplicant code)
- Growing support for supplicants in the industry
  - –Microsoft—native in Win2K, XP, and 2003
  - –Meetinghouse: Now Cisco CSSC —support for WinNT, Win2K, WinXP, Win98, WinME, Solaris, Red Hat Linux
  - –Opensource—Open1x xsupplicant for UNIX/Linux platforms
  - –Apple—native OS X support
  - –Cisco:
    - ACU: wireless client
    - CTA: wired client

Supplicant Considerations

- **Microsoft Windows**
  - User and machine authentication
  - DHCP request time out
  - Machine authentication restriction
  - Default methods : MD5, PEAP, EAP-TLS
- **Unix/Linux considerations**
  - Open source : xsupplicant Project (University of Utah)
  - Available from http://www.open1x.org
  - Supports EAP-MD5, EAP-TLS,
  - PEAP/MSCHAPv2, PEAP/EAP-GTC
- **Native Apple supplicant support in OS X 10.3**
  - 802.1x is turned off by default!
  - Default parameters—TTLS, LEAP, PEAP, MD5 supported
  - Support for airport and wired interfaces
  - Single sign on can be accomplished w/Applescripts
- **Commercial products Cisco CSSC**



Authorization

- Authorization is the embodiment of the ability to enforce policies on identities
- Typically policies are applied using a group methodology—allows for easier manageability
- The goal is to take the notion of group management and policies into the network
- The most basic authorization in 802.1x and IBNS is the ability to allow or disallow access to the network at the link layer
- Other forms of authorization include VLAN assignment, ACL assignment, QoS policy assignment, 802.1x with ARP inspection, etc.

802.1x with VLAN Assignment

AV Pairs Used—All Are IETF Standard

- [64] Tunnel-type—“VLAN” (13)
- [65] Tunnel-medium-type—“802” (6)
- [81] Tunnel-private-group-ID—<VLAN name>


```
IOS
aaa authorization network default group radius
```

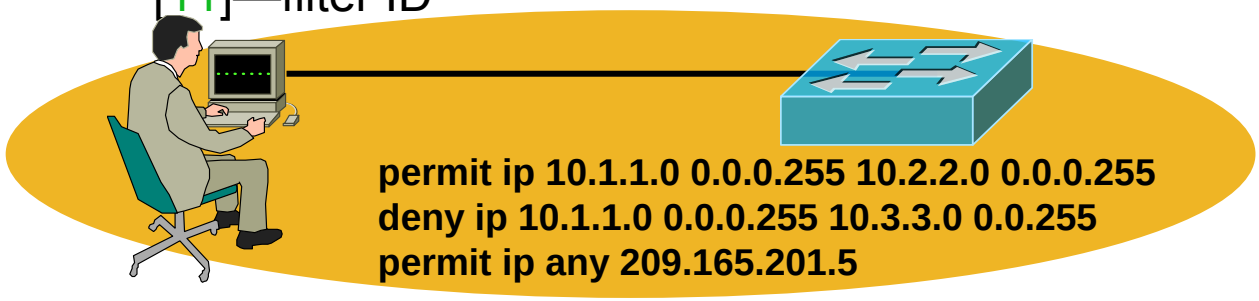
- VLAN name must match switch configuration
- Mismatch results in authorization failure

802.1x with VLAN Assignment

- Dynamic VLAN assignment based on identity of group, or individual, at the time of authentication
- VLANs assigned by name—allows for more flexible VLAN management
- Allows dynamic VLAN policies to be applied to groups of users (i.e., VLAN QoS, VLAN ACLs, etc.)
- Tunnel attributes used to send back VLAN configuration information to authenticator
- Tunnel attributes are defined by RFC 2868
- Usage for VLANs is specified in the 802.1x standard

802.1x with ACL Assignment

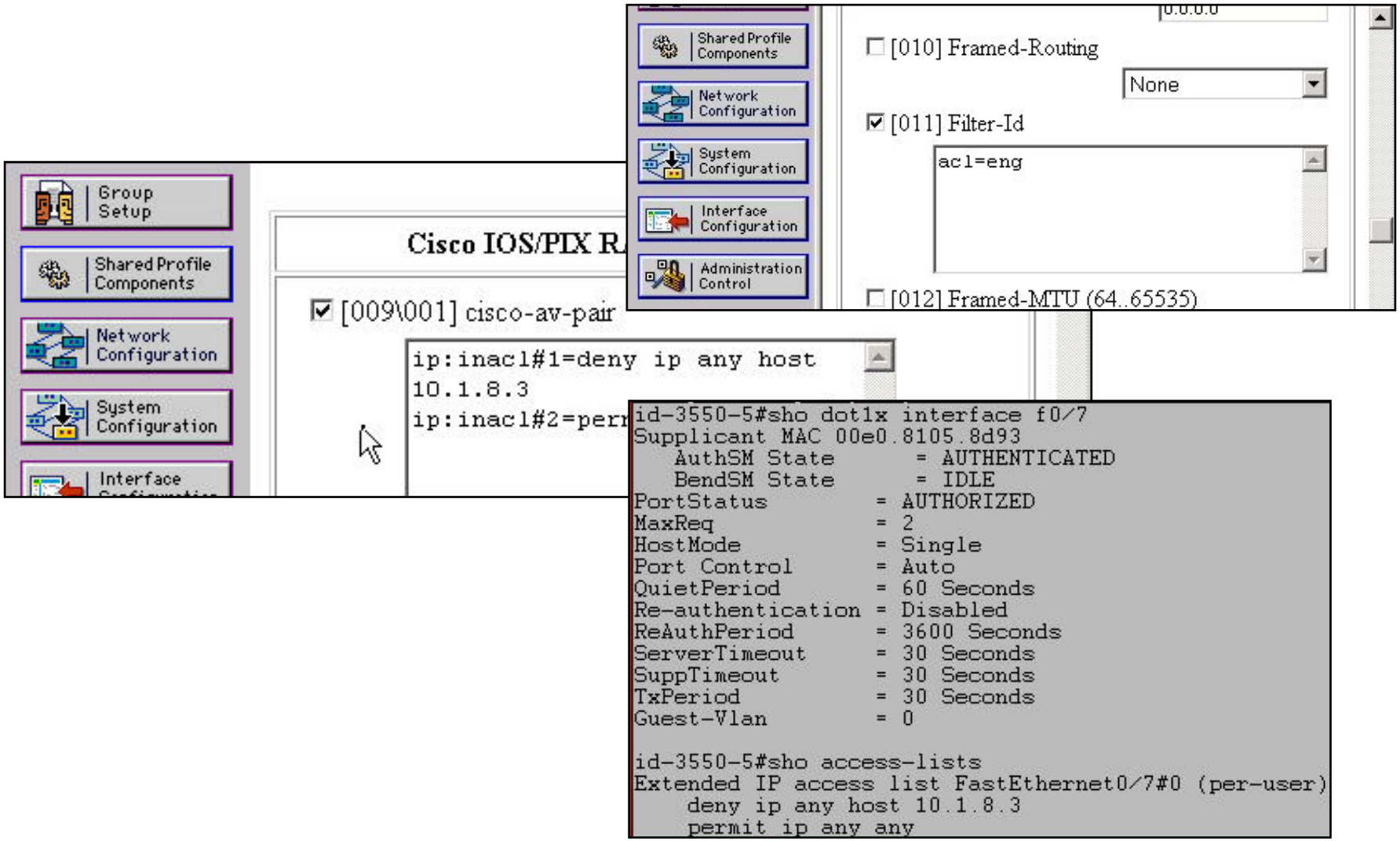
- Vendor-specific attributes used for RADIUS
  - [026]—vendor specific
  - [009]—vendor ID for Cisco
  - [001]—refers to the VSA number
- Attribute used for predefined ACLs
  - [11]—filter ID



IOS

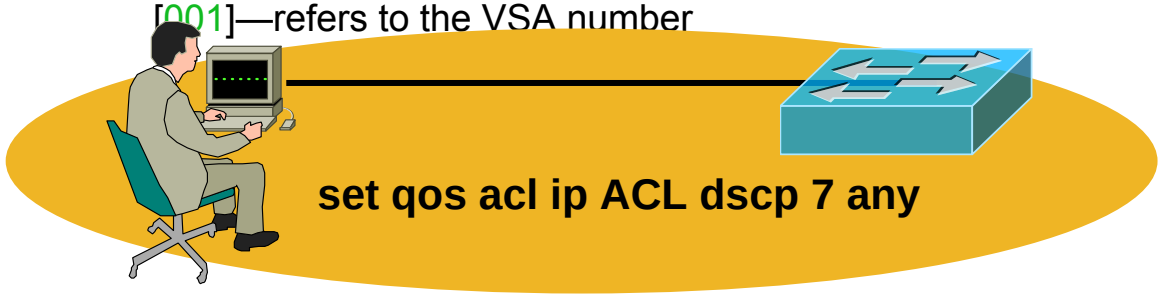
```
aaa authorization network default group radius
```

802.1x with ACLs



802.1x with QoS Policy

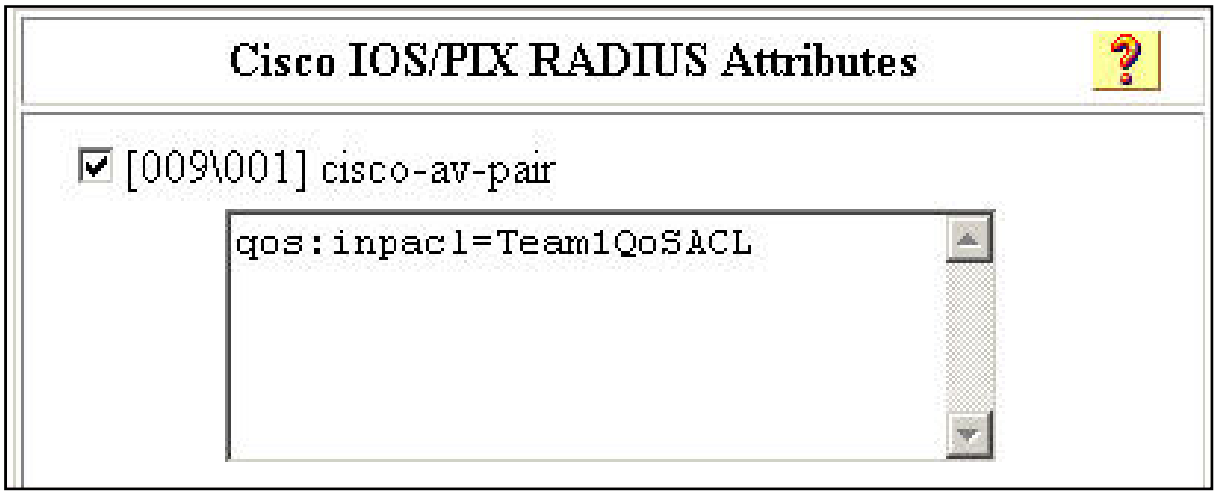
- Vendor-specific attributes used for RADIUS
  - [026]—vendor specific
  - [009]—vendor ID for Cisco
  - [001]—refers to the VSA number




```
IOS
aaa authorization network default group radius
```

- Use to enable the automatic QoS provisioning of users
- In this example, RADIUS will send down a QoSPACL name along with an accept packet
- Policy converted into ACEs and installed on this switch

802.1x with QoS Policy




```
id-switch> (enable)
id-switch> (enable) sho qos acl map runtime Team1QoSACL
QoS ACL mappings on input side:
ACL name                          Type Vlans
--------------------------------- ---- ---------------------------------
Team1QoSACL                         IP
ACL name                          Type Ports
--------------------------------- ---- ---------------------------------
Team1QoSACL                         IP 3/11
QoS ACL mappings on output side:
ACL name                          Type Vlans
--------------------------------- ---- ---------------------------------
Team1QoSACL                         IP
id-switch> (enable)
```

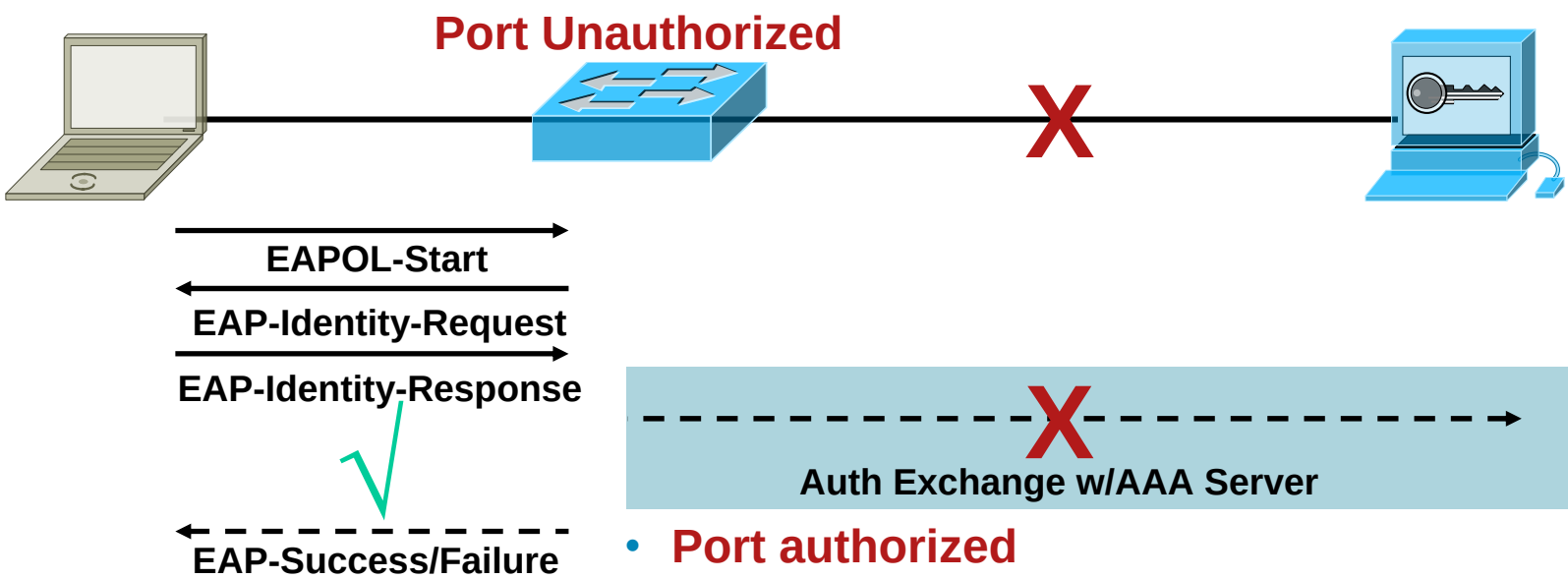
- DEMO 802.1x avec Dyn VLAN assignment, ACL et QoS **Déployment de la QoS sur le port du commutateur (avec et sans worm...)**
- (un ou l'autre ou les deux)

802.1x and Authorization Failure

- The switch will fail authentication to a client if authorization from the authentication server cannot be applied to the switch
- For example, vlan = employee and there is no vlan named employee on the switch
- Issue is exacerbated with NAC2 since CTA pop up says healthy, ACS says healthy, the switch fails the authentication, and client shows a failed authentication

Inaccessible Authentication Bypass

```
IOS
Dot1x critical
radius-server x.x.x.x username test password test
Interface gigabitethernet 1/0/1
 dot1x critical
 dot1x critical vlan 10
```

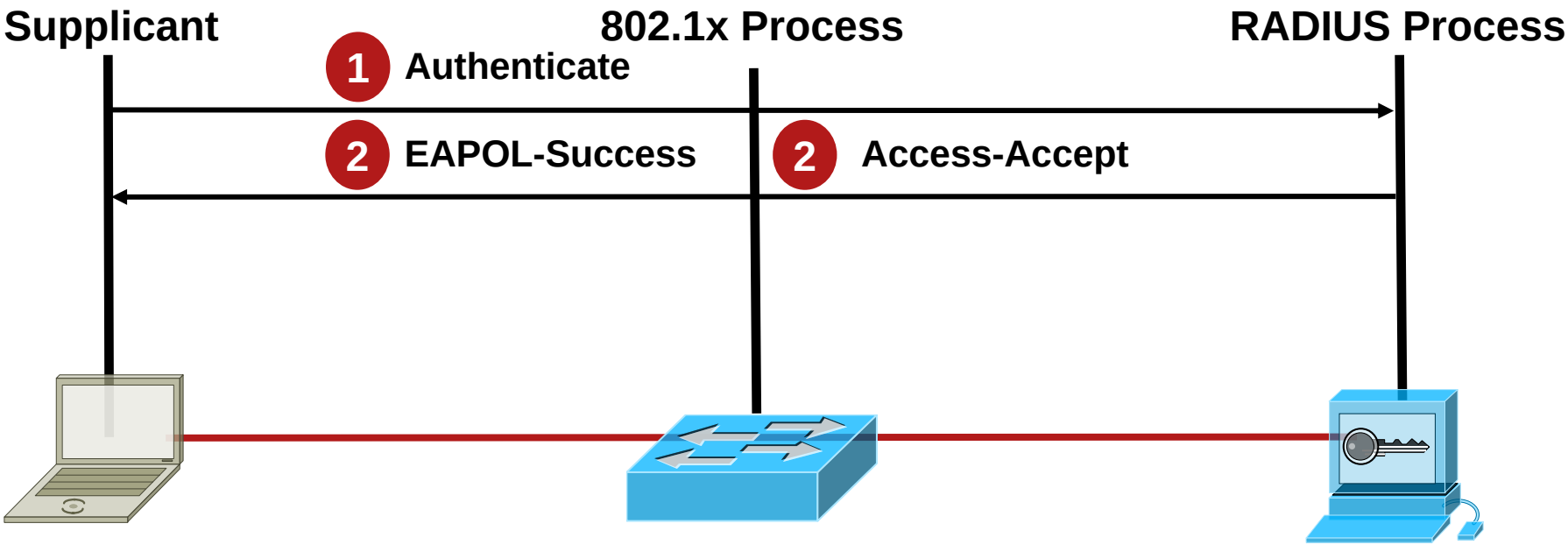


- Port authorized
- Move to access VLAN (first authentication)
- Or keep existing VLAN (re-authentication)

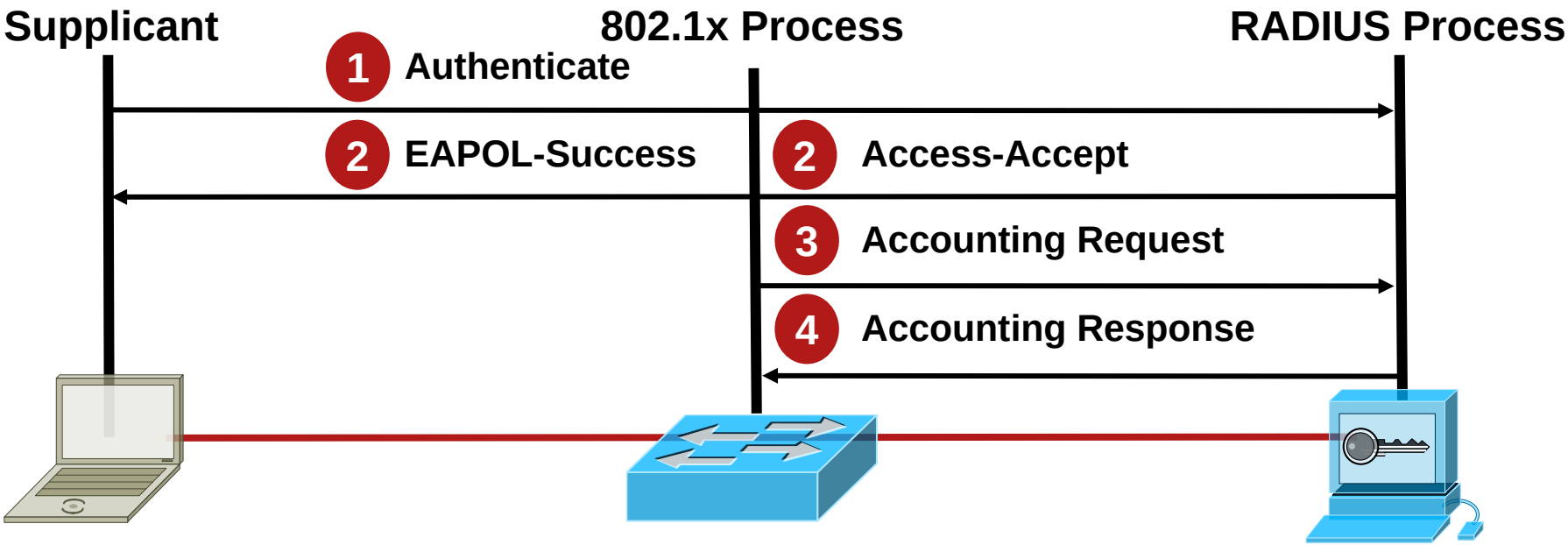
IBNS Reporting and Monitoring

- Major components to IBNS monitoring
  - RADIUS accounting
  - NAD logs
  - RADIUS logs
  - NAD CLI
- Major components of IBNS reporting
  - Correlated log reports (MARS)

802.1x with RADIUS Accounting



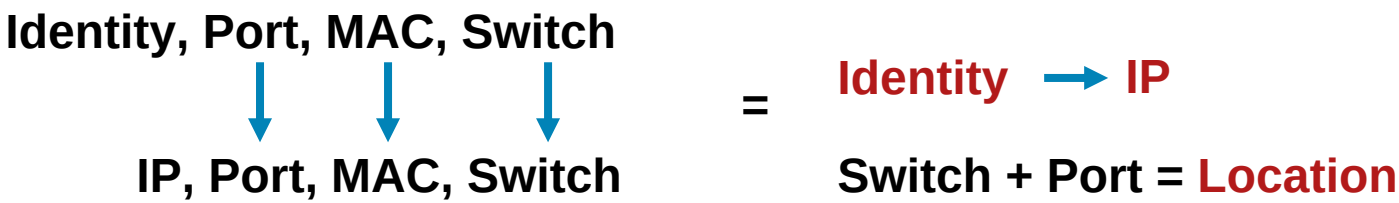
802.1x with RADIUS Accounting



- Accounting-request packets
- Contains one or more AV pairs to report various events and related information to the RADIUS server
- Tracking user-level events are used in the same mechanism

802.1x with RADIUS Accounting

- Similar to other accounting and tracking mechanisms that already exist using RADIUS
  - Can now be done through 802.1x
- Increases network session awareness
- Provide information into a management infrastructure about who logs in, session duration, support basic billing usage reporting, etc.
- Provides a means to map the information of authenticated



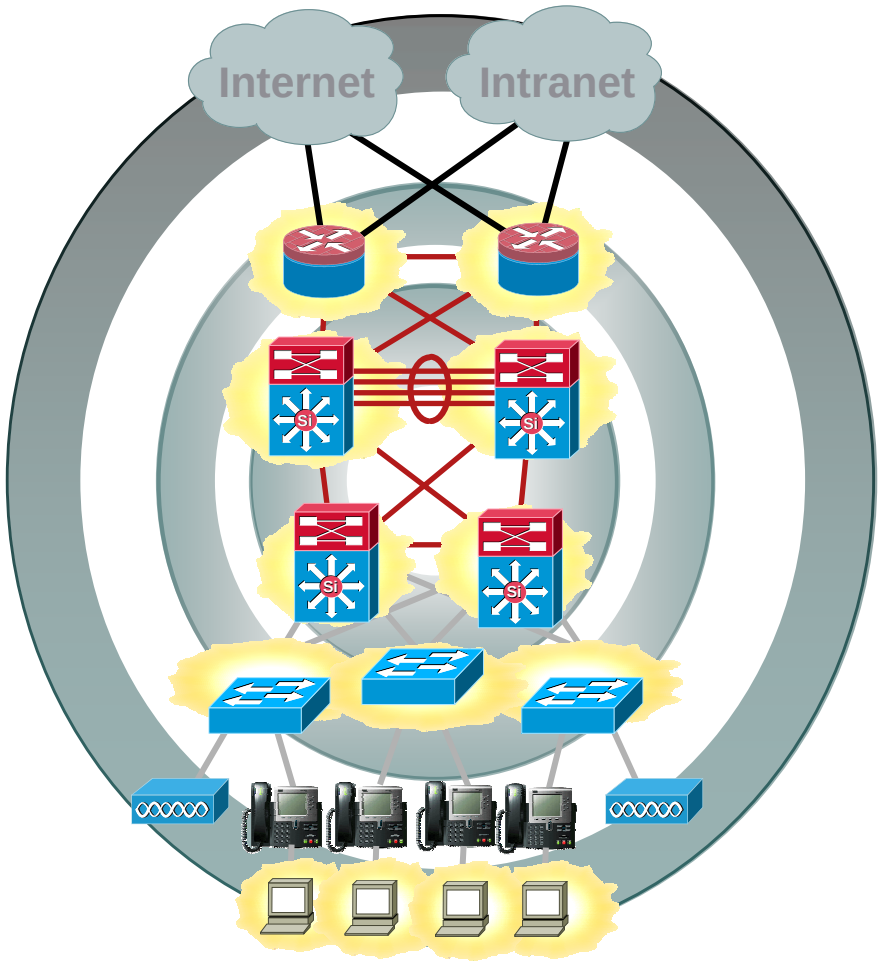

```
IOS
aaa accounting dot1x default start-stop group radius
```

Demo Accounting 802.1x

Fin section Sylvain D

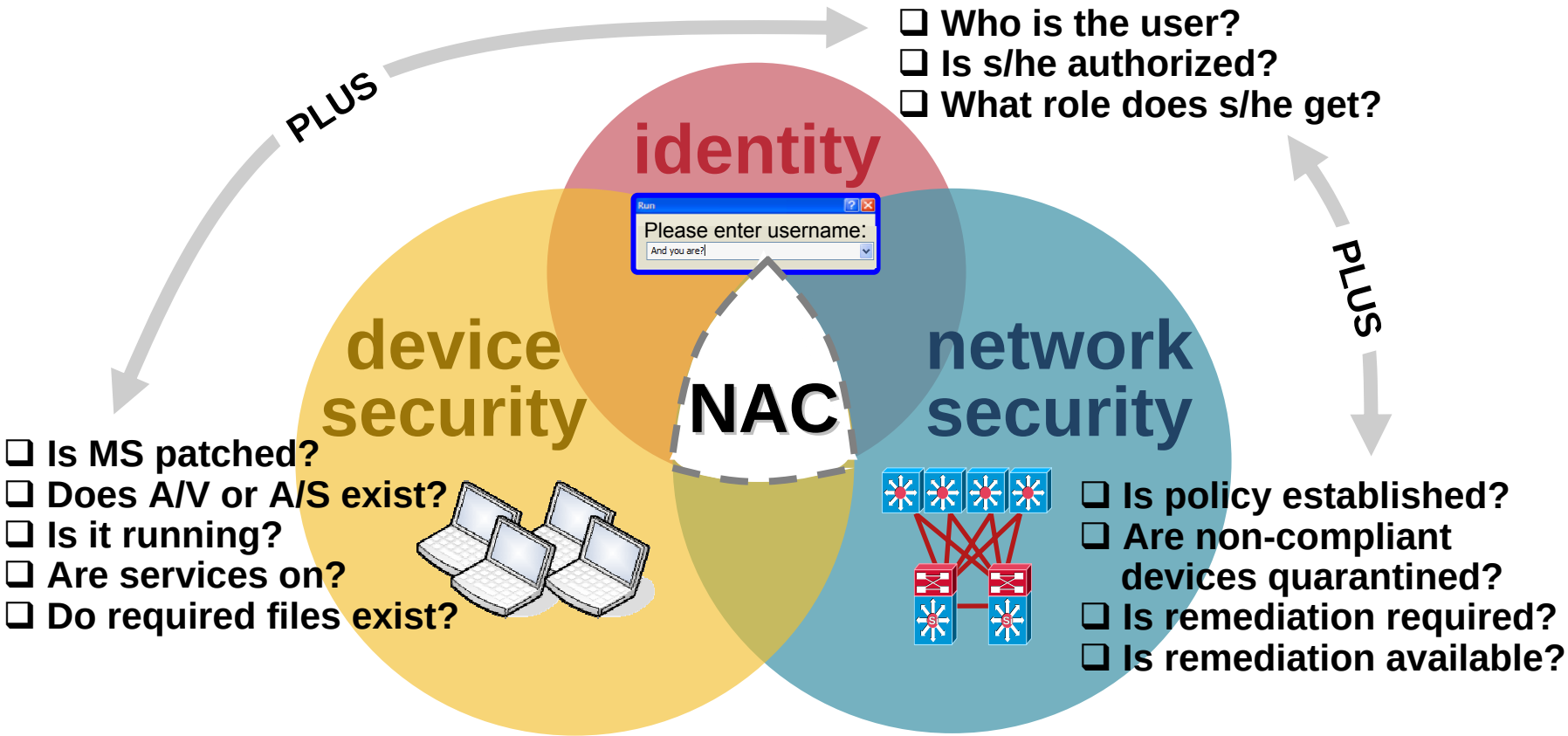
Programme

- Authentification
  - Qui peut accéder le réseau
  - L'impact de la téléphonie
  - 802.1x, les visiteurs, Web Base . Authentification
- La conformité des postes au moment de la connexion
  - Sur le LAN, en VPN, etc...
- Les bonnes pratiques pour le contrôle des usagers connectés au réseau
  - Fonctions de sécurité présentent dans les commutateurs Cisco
  - QoS déployée?
  - Cisco Securité Agent (CSA)
- La surveillance et la configuration du réseau



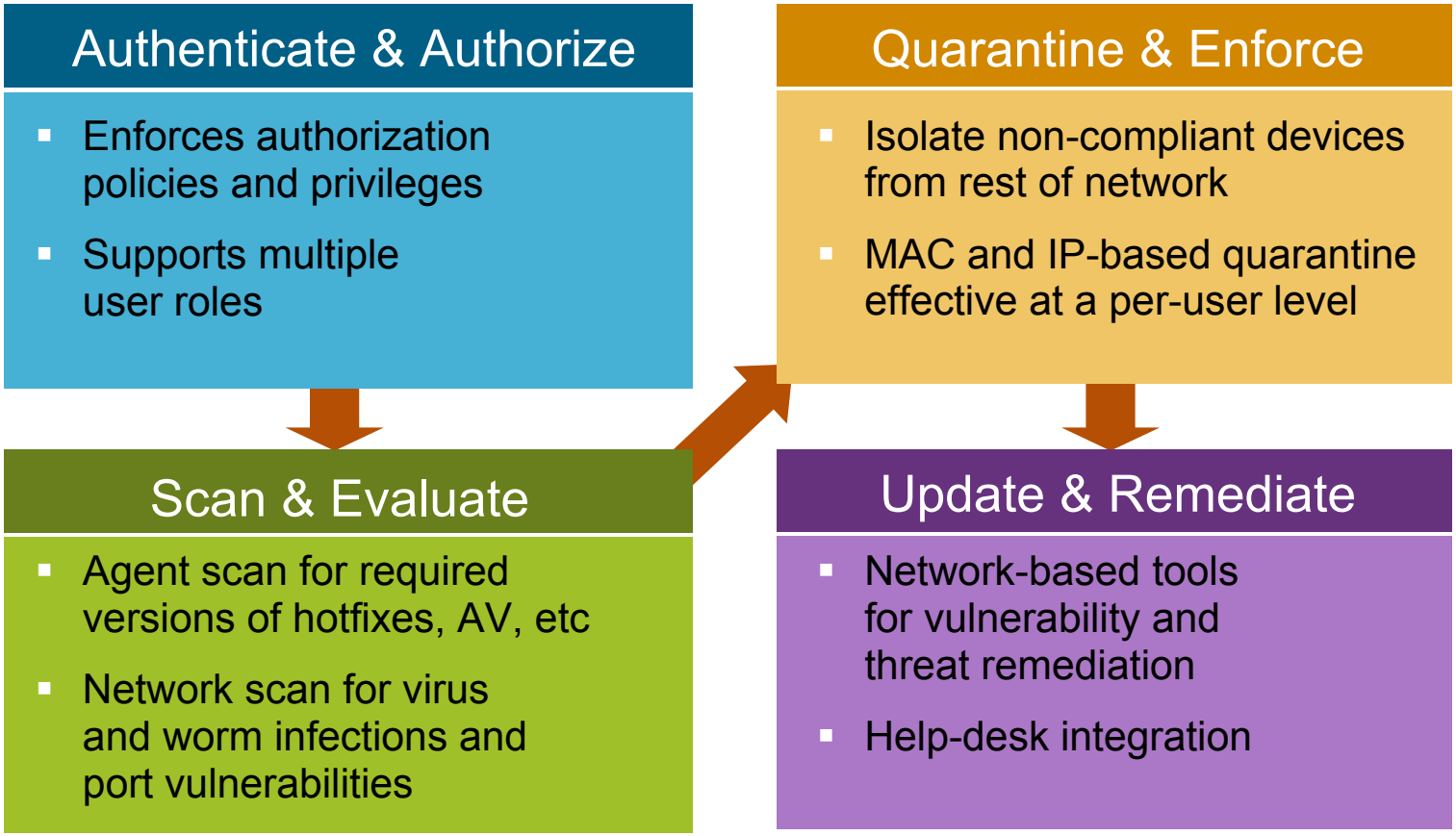
What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.



Make Access Contingent on Compliance

First, establish ACCESS POLICIES. Then:



NO COMPLIANCE = NO NETWORK ACCESS

NAC Means Better Criteria for Security

What System Is It?	**Windows, Mac or Linux** **Laptop or Desktop or PDA** **Printer or Other Corporate Asset**
Who Owns It?	**Company** **Employee** **Contractor** **Guest** **Unknown**
Where Is It Coming From?	**VPN** **LAN** **WLAN** **WAN**
What's On It? **Is It Running?**	**Anti-Virus, Anti-Spyware** **Personal Firewall** **Patching Tools**
What's The Preferred Way To Check/Fix It?	**Pre-Configured Checks** **Customized Checks** **Self-Remediation or Auto-Remediation** **Third-Party Software**

Four Key Capabilities of Cisco NAC

	Securely Identify Device and User	Enforce Consistent Policy	Quarantine and Remediate	Configure and Manage
What It Means	Associate Users to Devices	Assess Devices; Enforce Policies	Isolate and Fix Non-compliant Devices	Create and Manage Policies Easily
Why It Is Important	Associating Users with Devices Enables Granular Enforcement of Policies by Role or group	Enforcement at the Network Reduces Reliance on the Integrity of the Endpoint	Quarantine Critical to Halt Spread of Vulnerabilities; Remediation Addresses Root Cost Drivers	Policies That Are Easy to Create and Maintain Lead to Better System Operations and Adherence

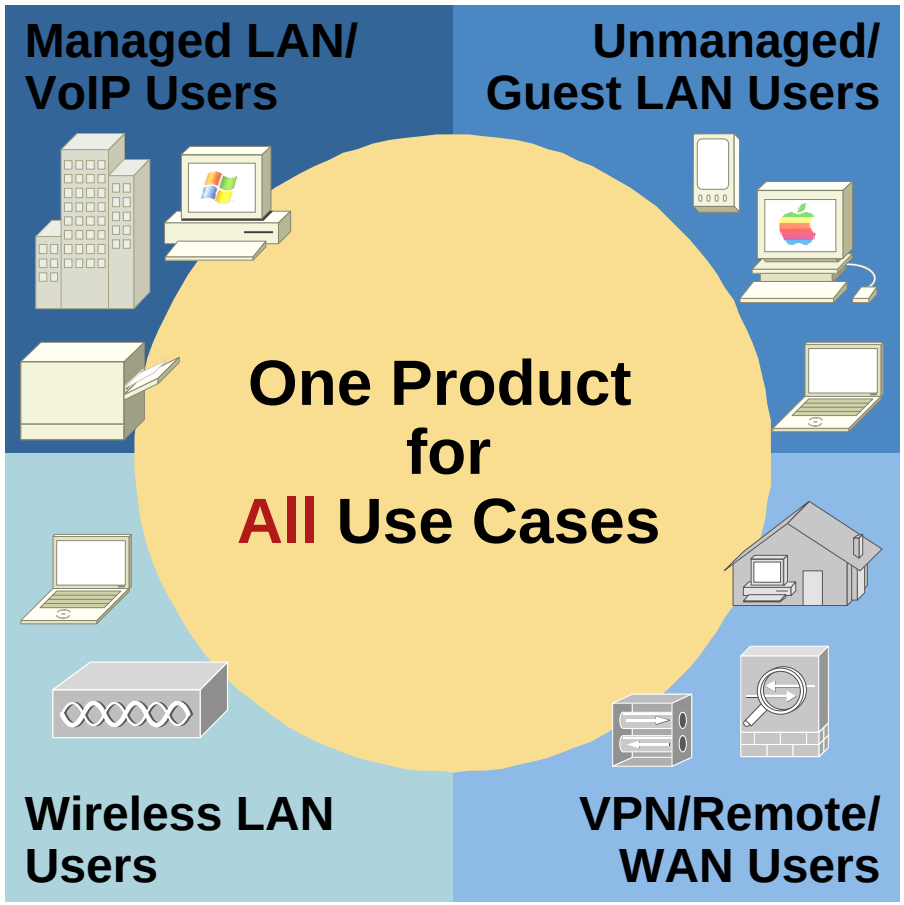
A *Comprehensive* NAC Solution Must Have All Four Capabilities: The Absence of Any One Weakens the Solution

Cisco NAC Is Widely Deployed Today

- NAC Appliance has 1500+ customers worldwide
- Mid-market and large enterprises
  - Financial services
  - Healthcare/Manufacturing
  - Public Sector
- All use cases
  - Remote Access
  - Wireless/Guest
  - Campus LAN

"Cisco.. is unrivaled as a market leader in the NAC appliance space, holding over 45% of the market."

-- Frost & Sullivan, 11/06



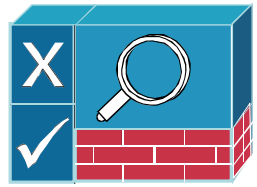
NAC Appliance Components

- Cisco Clean Access Manager

  Centralizes management for administrators, support personnel, and operators

- Cisco Clean Access Server

  Serves as enforcement point for network access control

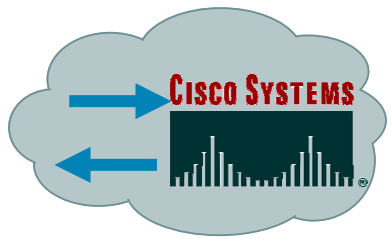


- Cisco Clean Access Agent

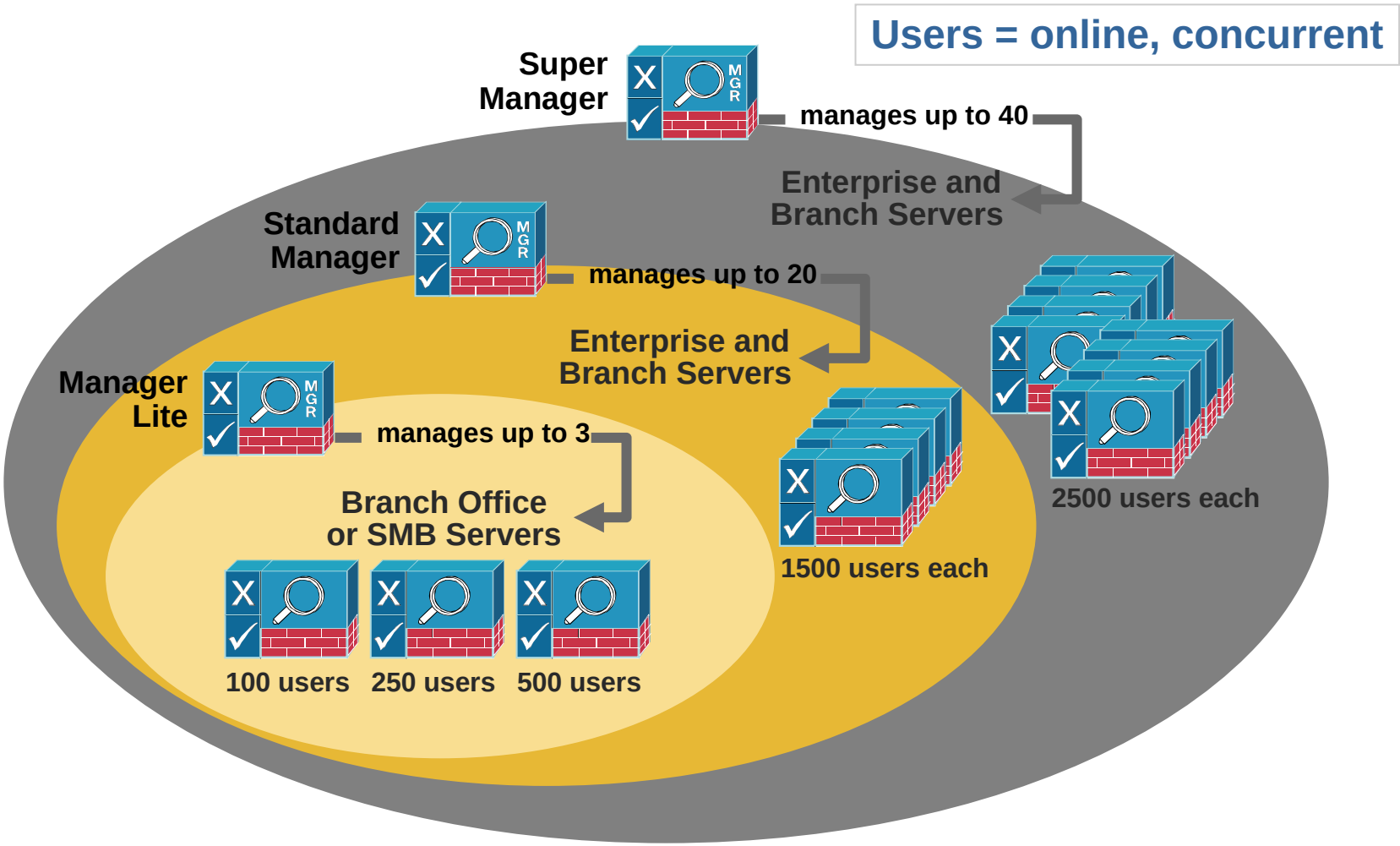
  Optional lightweight client for device-based registry scans in unmanaged environments

- Rule-set Updates

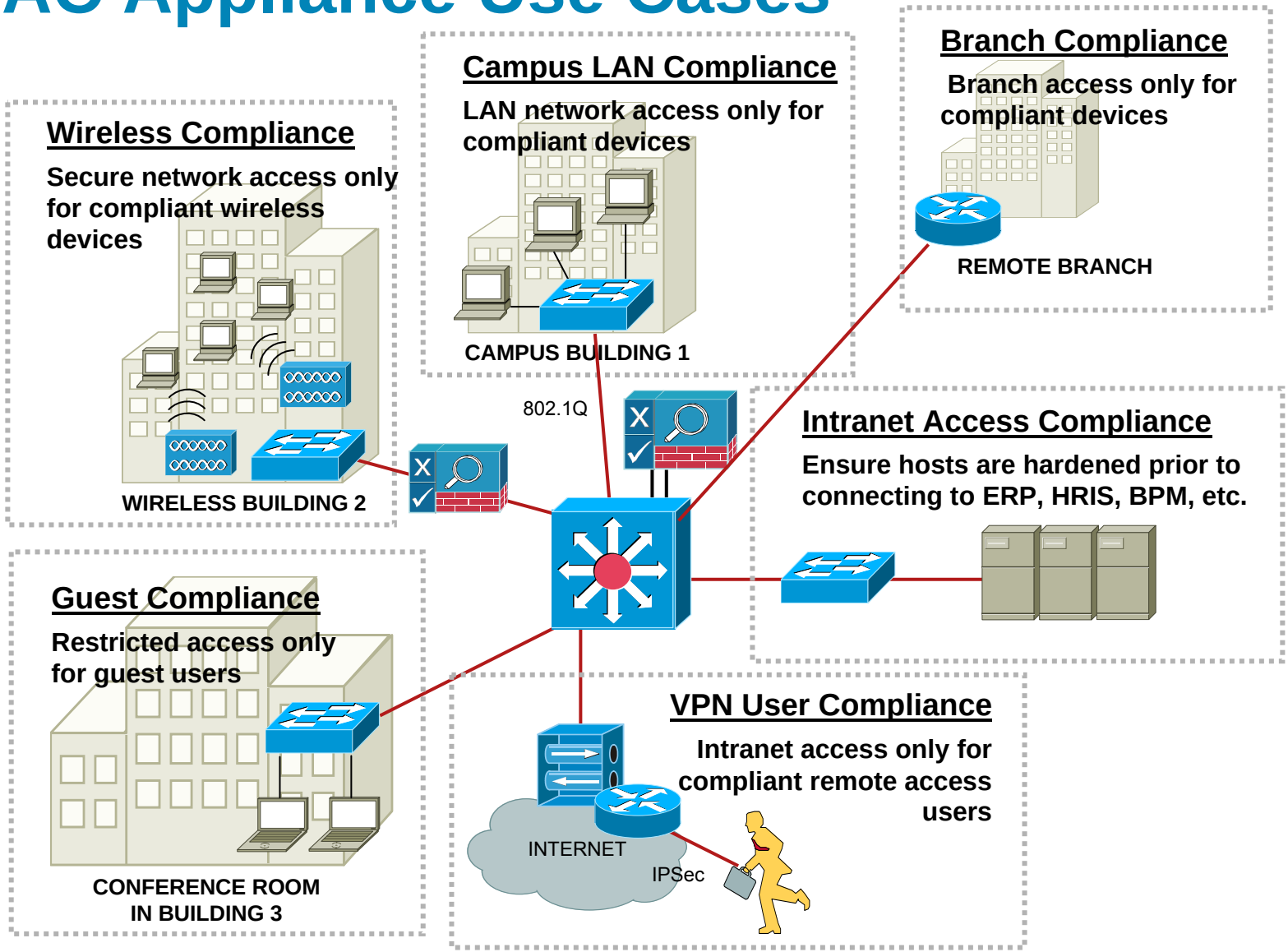
  Scheduled automatic updates for anti-virus, critical hot-fixes and other applications



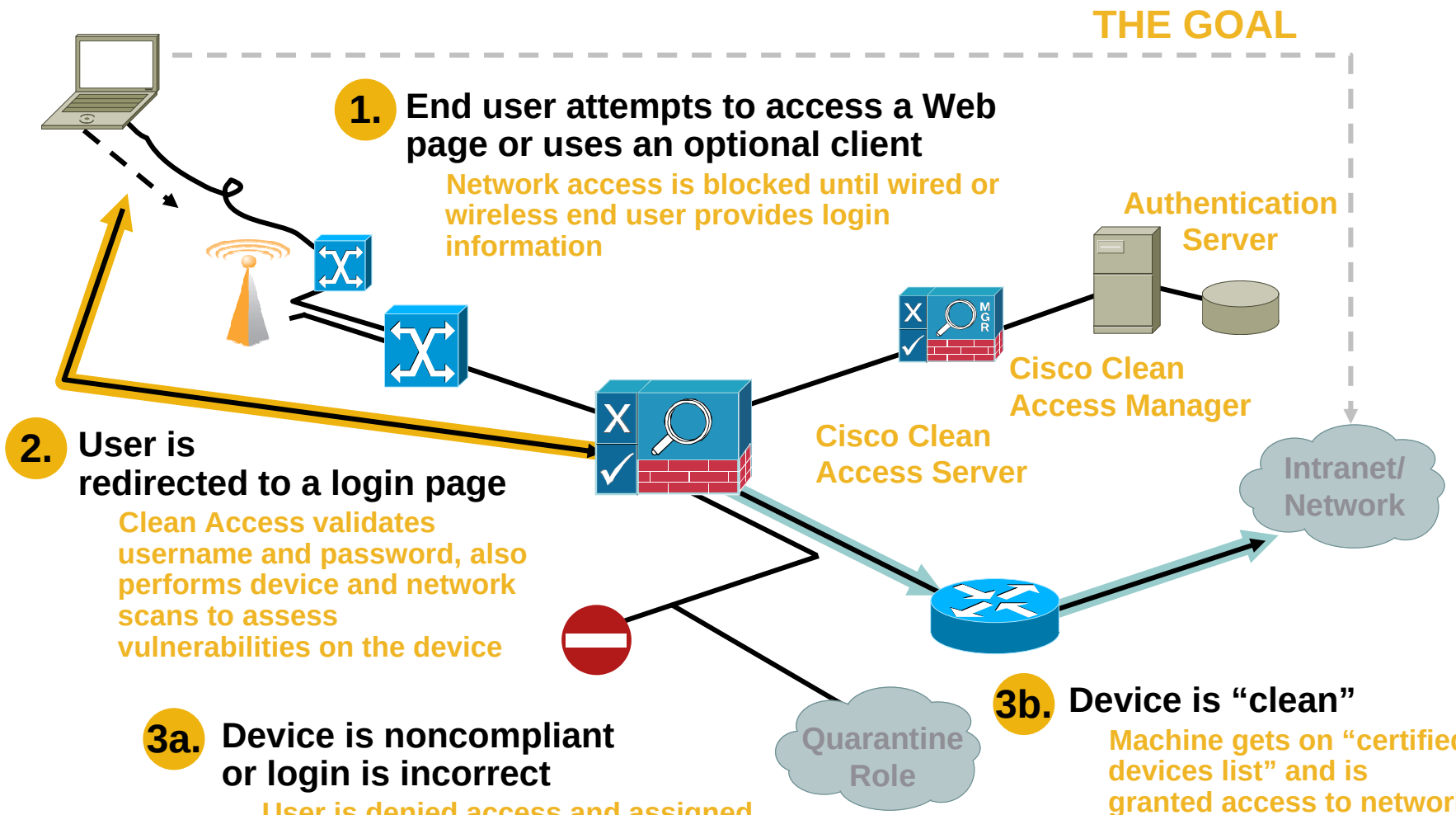
NAC Appliance Sizing



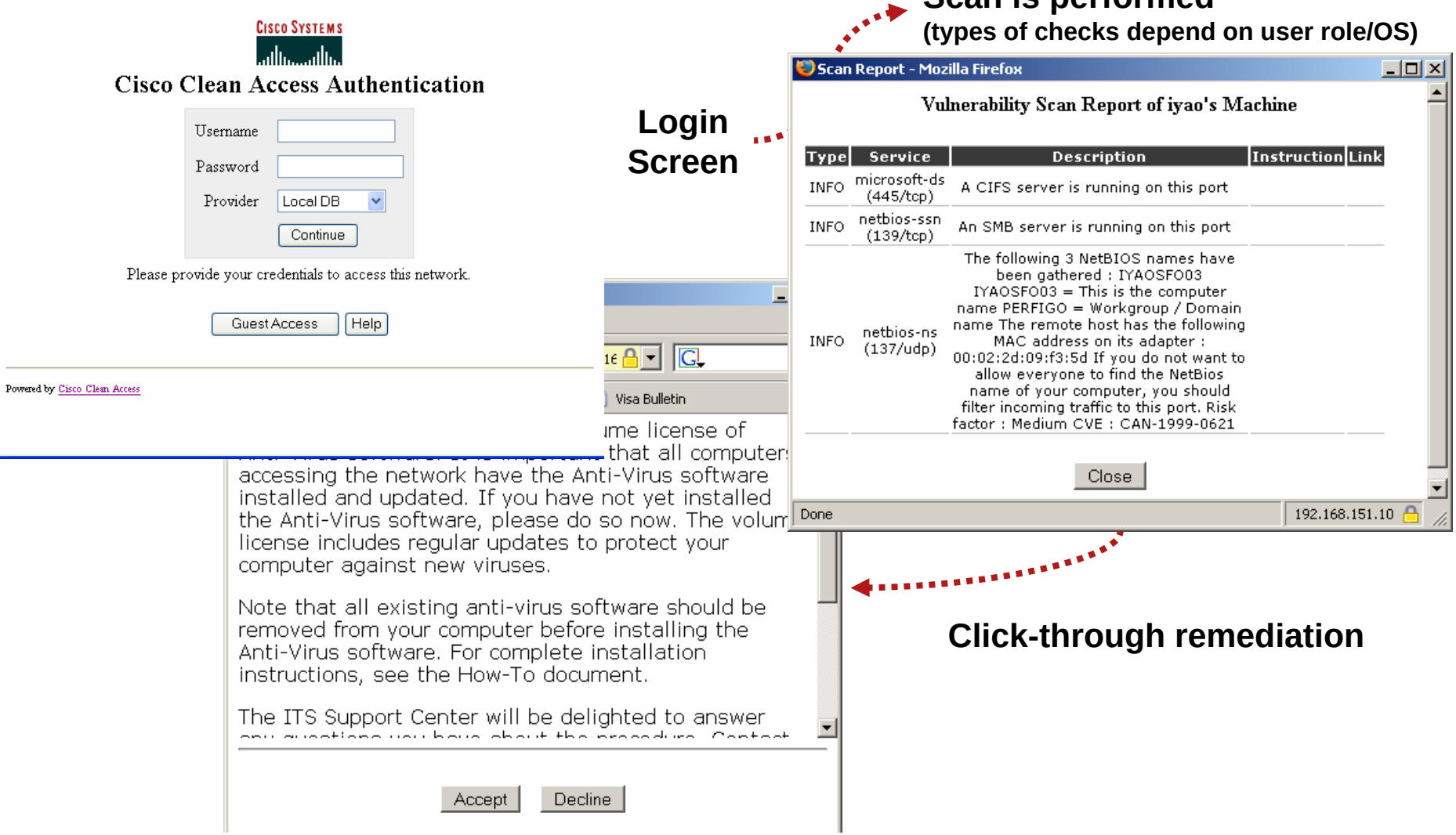
NAC Appliance Use Cases



Cisco NAC Appliance Overview



End User Experience: Web-based



End User Experience: Web-based

Flash Demo - cca_agentless_swf_v3.swf

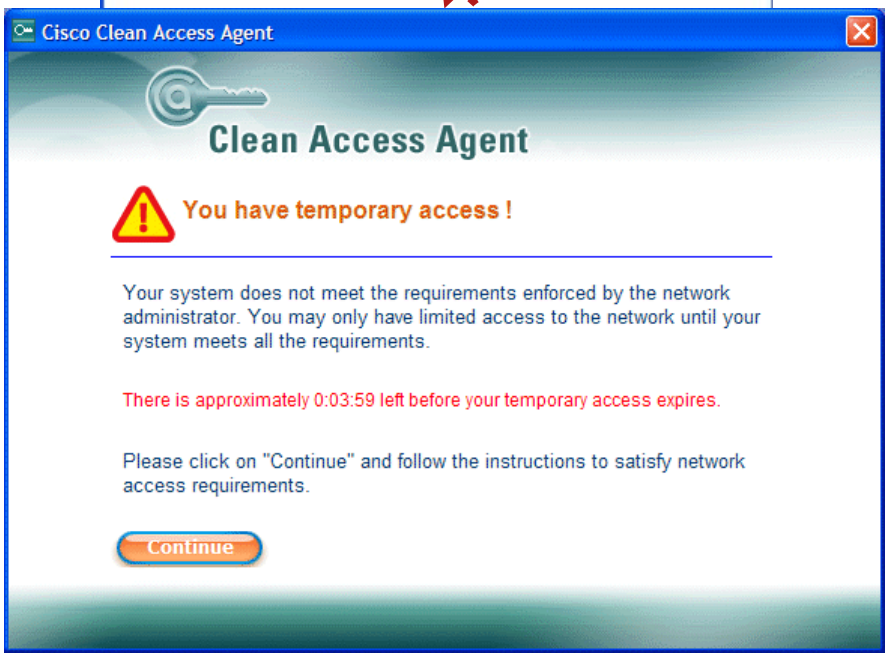
End User Experience: with Agent

Login Screen

Scan is performed
(types of checks depend on user role)

Scan fails

Remediate



End User Experience: with Agent

Flash Demo - cca_inline_agent_sso_swf_v1.swf

Cisco NAC Appliance Partnerships

Cisco NAC is committed to protecting customer's investments in partner applications

NAC Appliance Supports Policies for 300+ Applications, Including these Vendors:

Corporate/Employee Posture Assessment

Corporate Asset Tag

- Unique registries inserted into corporate devices
- Corporate PKI certificates installed in corporate devices

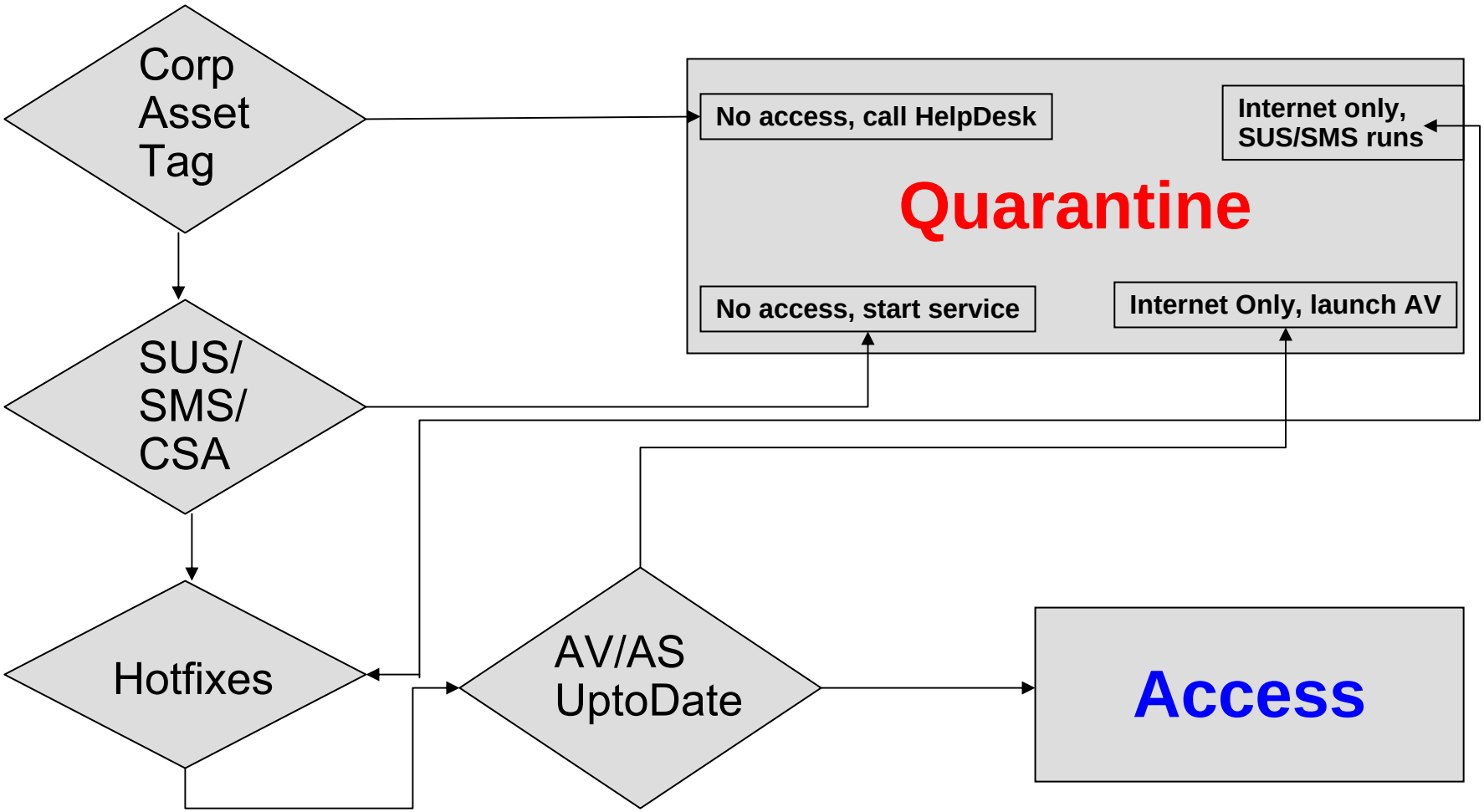
Microsoft Hotfixes:

- Critical hot-fixes checks (provided via Cisco automated updates)
- SUS/WUS running or AU Options (can force setting)
- Patch Management SW running (can launch qualified .exe)

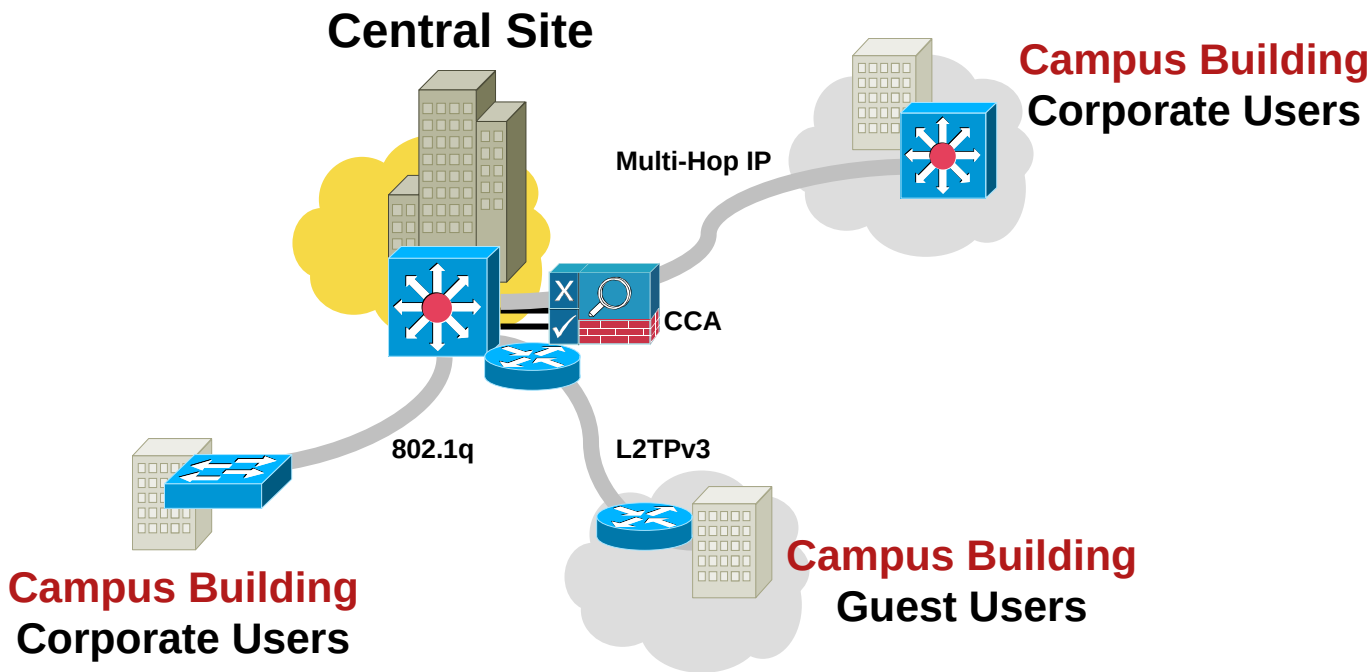
Security Applications:

- HIDS (CSA) or Personal Firewall installed and running
- AV installed, running and latest DAT (can launch AV)
- Anti-Spyware installed and running
- Encryption software installed and running

NAC Decision Tree for Employee

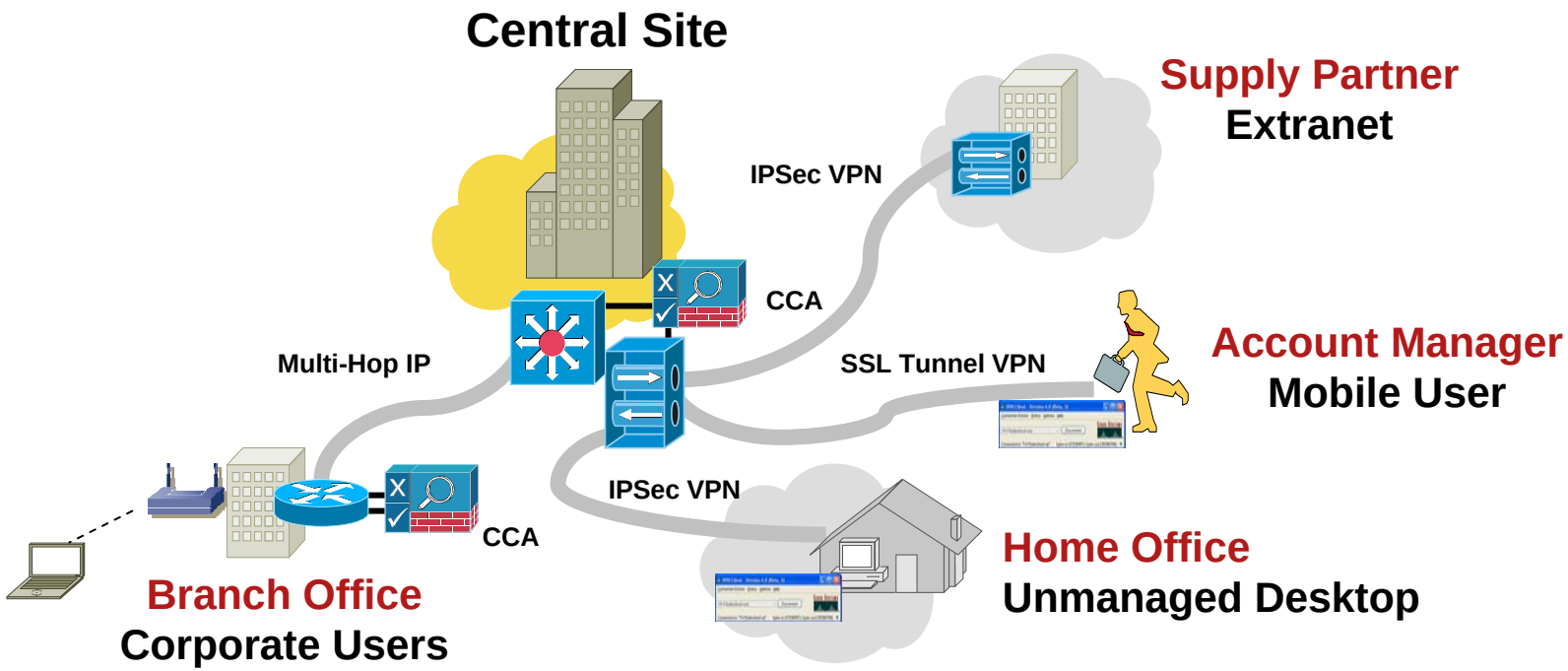


Cisco Clean Access for Corporate LAN



FEATURES	BENEFITS
▪ Supports 802.1q trunking ▪ Supports both L3 multi-hop and L2 ▪ Supports L2TPv3 tunneling ▪ Supports both inband and out-of-band	▪ Enables central deployment mode ▪ End user devices can be several hops away ▪ Extends enforcement to campus buildings ▪ Leverages AD SSO

Cisco Clean Access for Remote Users

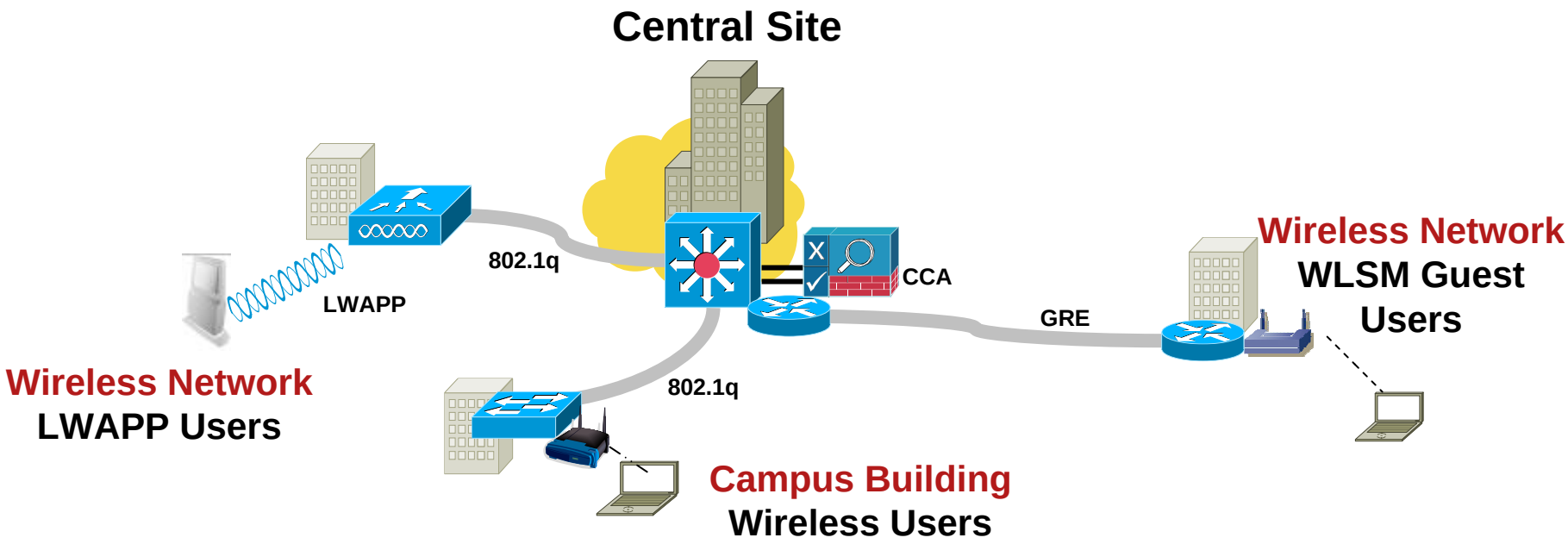


FEATURES	BENEFITS
▪ Supports IPSec and SSL Tunnel VPNs ▪ Supports site-to-site VPNs ▪ Supports VPN user sign-on	▪ Extends policy enforcement and compliance to remote access and VPN users ▪ Extends enforcement to site-to-site VPN partners ▪ Leverages VPN sign-on for single-sign-on

End User Experience: Remote Access

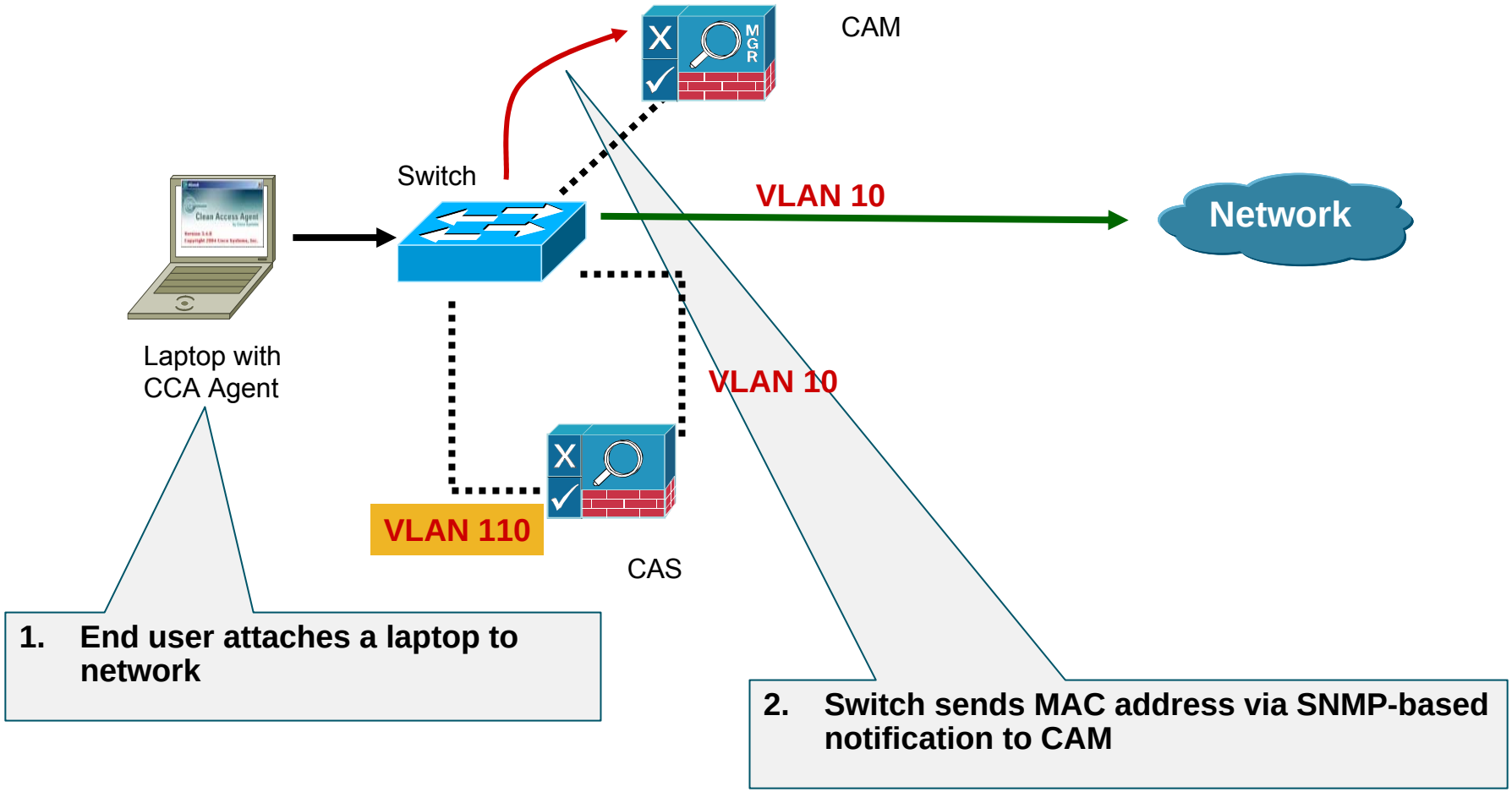
Flash Demo - cca_ssl_vpn_swf_v1.swf

Cisco Clean Access for Wireless Users

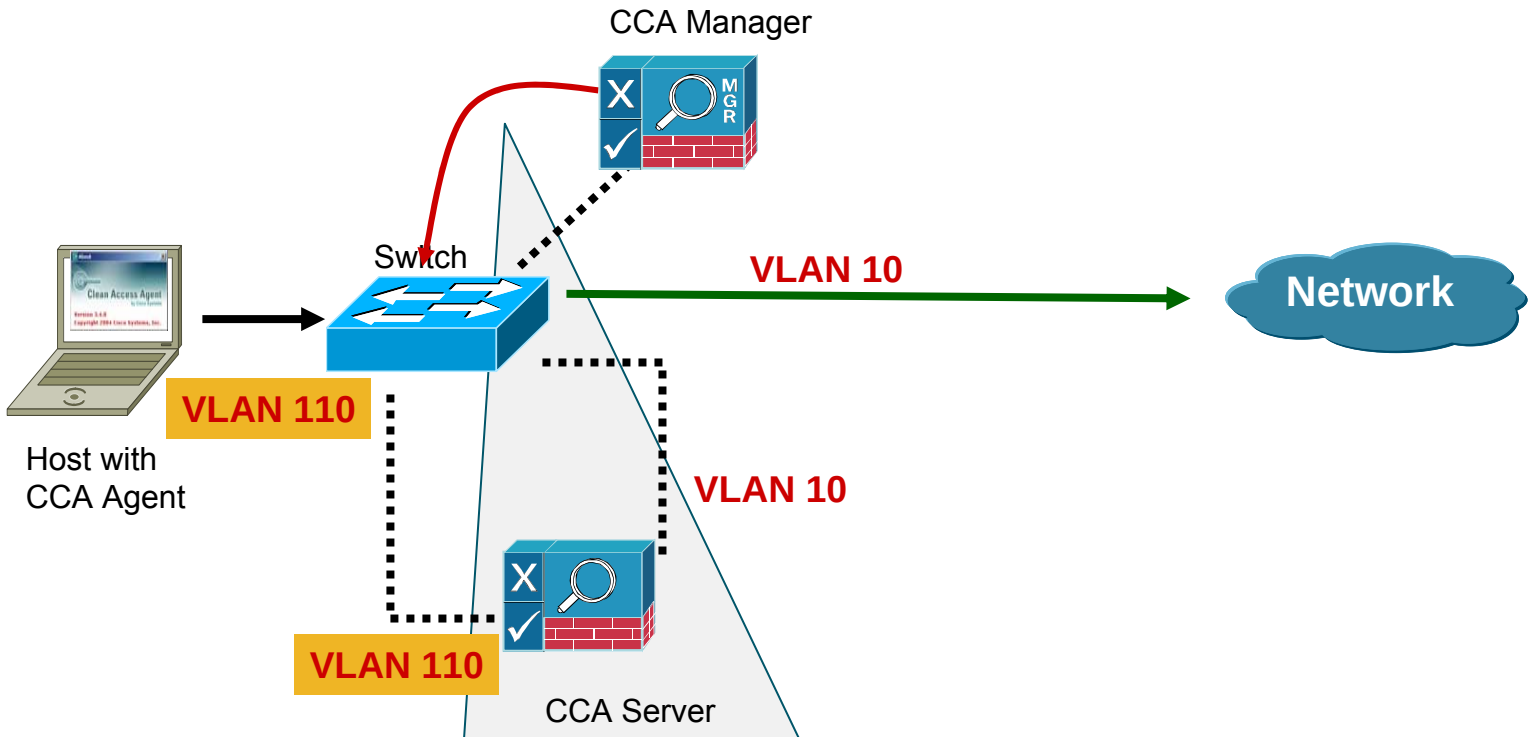


FEATURES	BENEFITS
▪ Supports 802.1q trunking ▪ Support L2TPv3 or GRE tunneling ▪ Supports thin or thick wireless 802.11 APs ▪ Supports Wireless user sign-on	▪ Enables central deployment mode ▪ End user devices can be several hops away ▪ Extends enforcement to any wireless networks ▪ Leverages EAP sign-on for single-sign-on

NAC Appliance Process Flow
Out-Of-Band Access

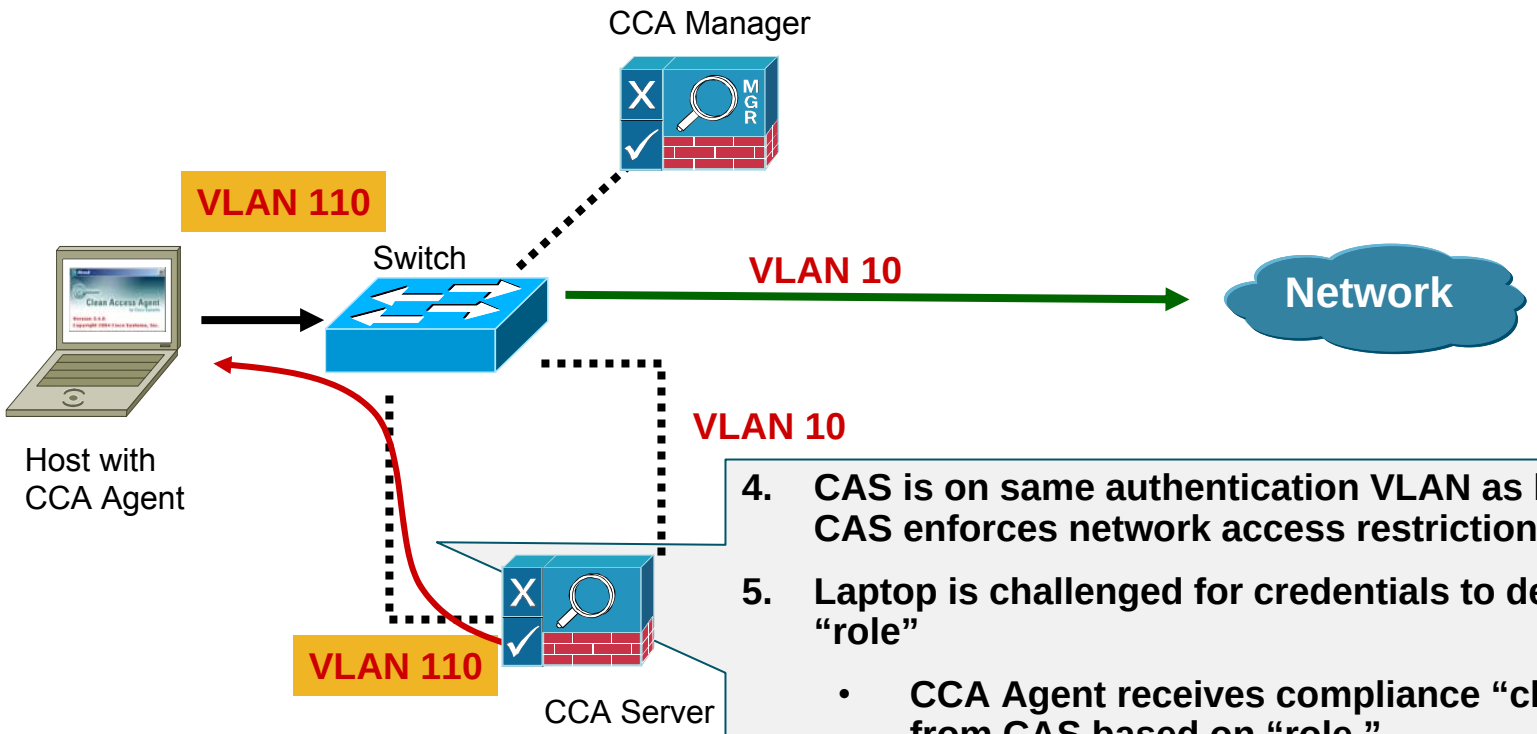


NAC Appliance Process Flow
Out-Of-Band Access



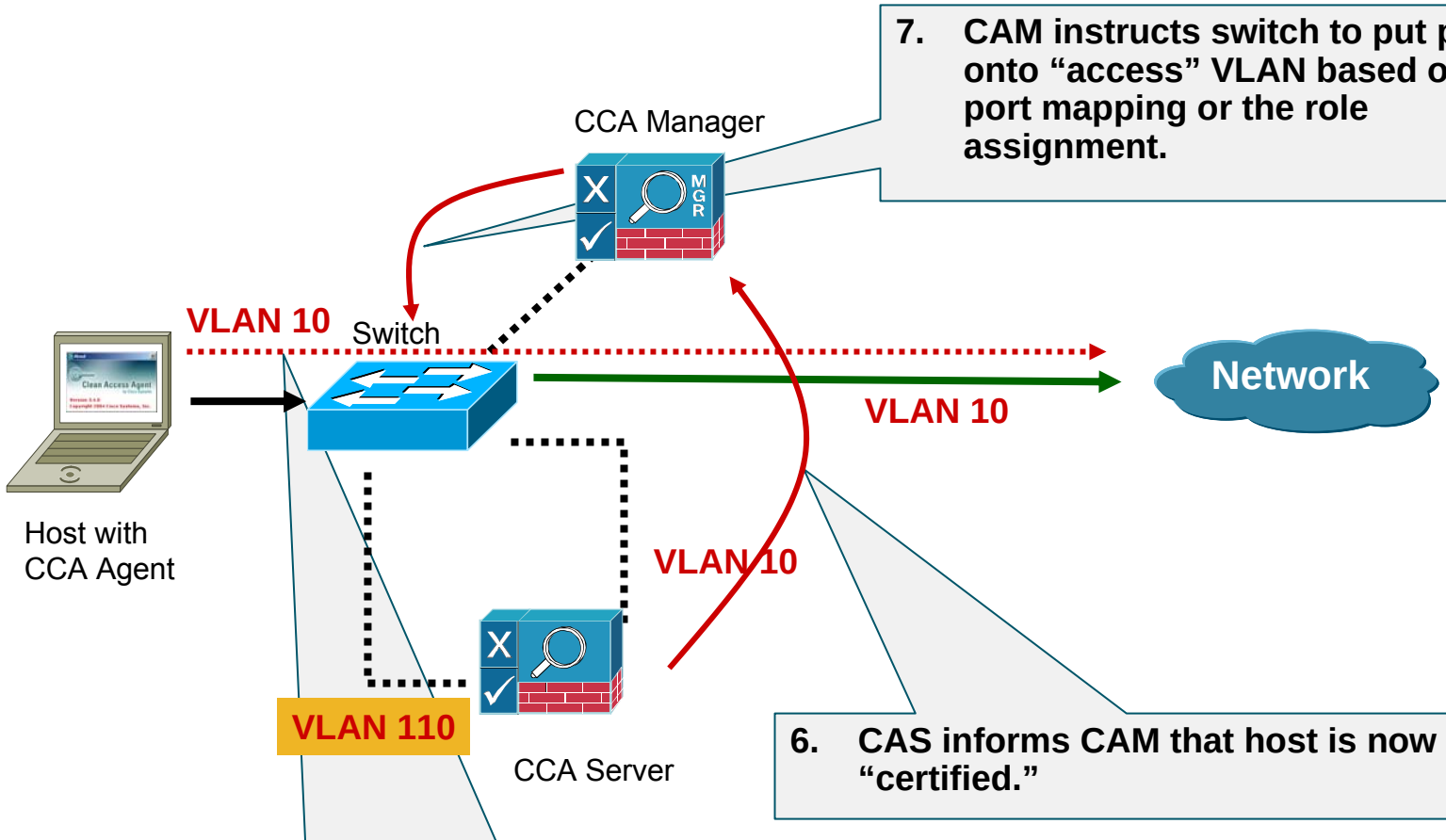
3. **CAM verifies if laptop is on the "OOB online" or "Certified devices" lists.**
   - **If the laptop is not in the "OOB online" or "Certified devices" list, the CAM instructs switch to assign port to authentication VLAN.**
   - **DHCP addressed is assigned as DHCP/DNS traffic traverses the CAS using VLAN mapping.**

NAC Appliance Process Flow
Out-Of-Band Access



4. **CAS is on same authentication VLAN as laptop. CAS enforces network access restriction.**
5. **Laptop is challenged for credentials to determine "role"**
   - **CCA Agent receives compliance "checks" from CAS based on "role."**
- **CCA Agent guides host through a step by step remediation process.**
  - **User allowed access to remediation sites enforced by CAS.**

NAC Appliance Process Flow
Out-Of-Band Access

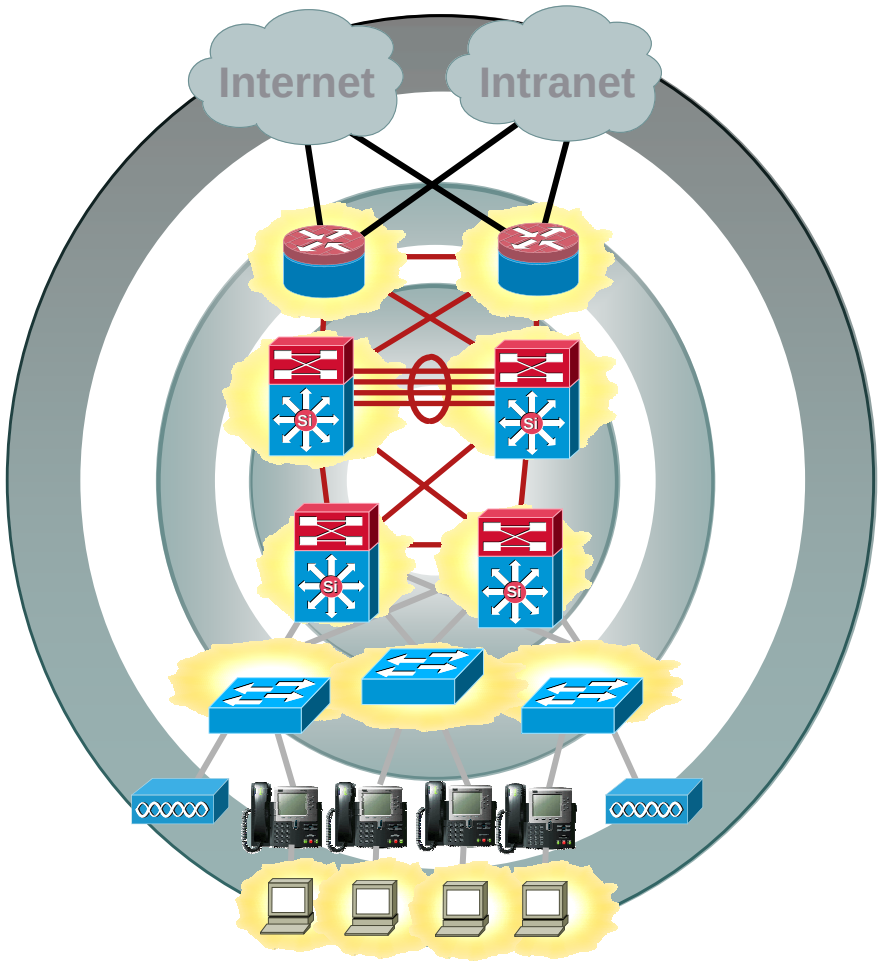


NAC Appliance Process Flow
Out-Of-Band Access

Flash Demo - cca_oob_agent_sso_swf_v1.swf

Programme

- Authentification
  - Qui peut accéder le réseau
  - L'impact de la téléphonie
  - 802.1x, les visiteurs, Web Base . Authentification
- La conformité des postes au moment de la connexion
  - Sur le LAN, en VPN, etc...
- Les bonnes pratiques pour le contrôle des usagers connectés au réseau
  - Fonctions de sécurité présentent dans les commutateurs Cisco
  - QoS déployée?
  - Cisco Securité Agent (CSA)
- La surveillance et la configuration du réseau



Catalyst Access Control Lists

What It Does:

Allows or denies access based on the source or destination address.

Restricts users to designated areas of the network, blocking unauthorized access to all other applications and information.

Benefits:

Prevents unauthorized access to servers and applications.

Allows designated users to access specified servers.

PACL - Provides granular control for limited access by the access port of the device

RACL - Controls traffic on Layer 2 and 3 interfaces.

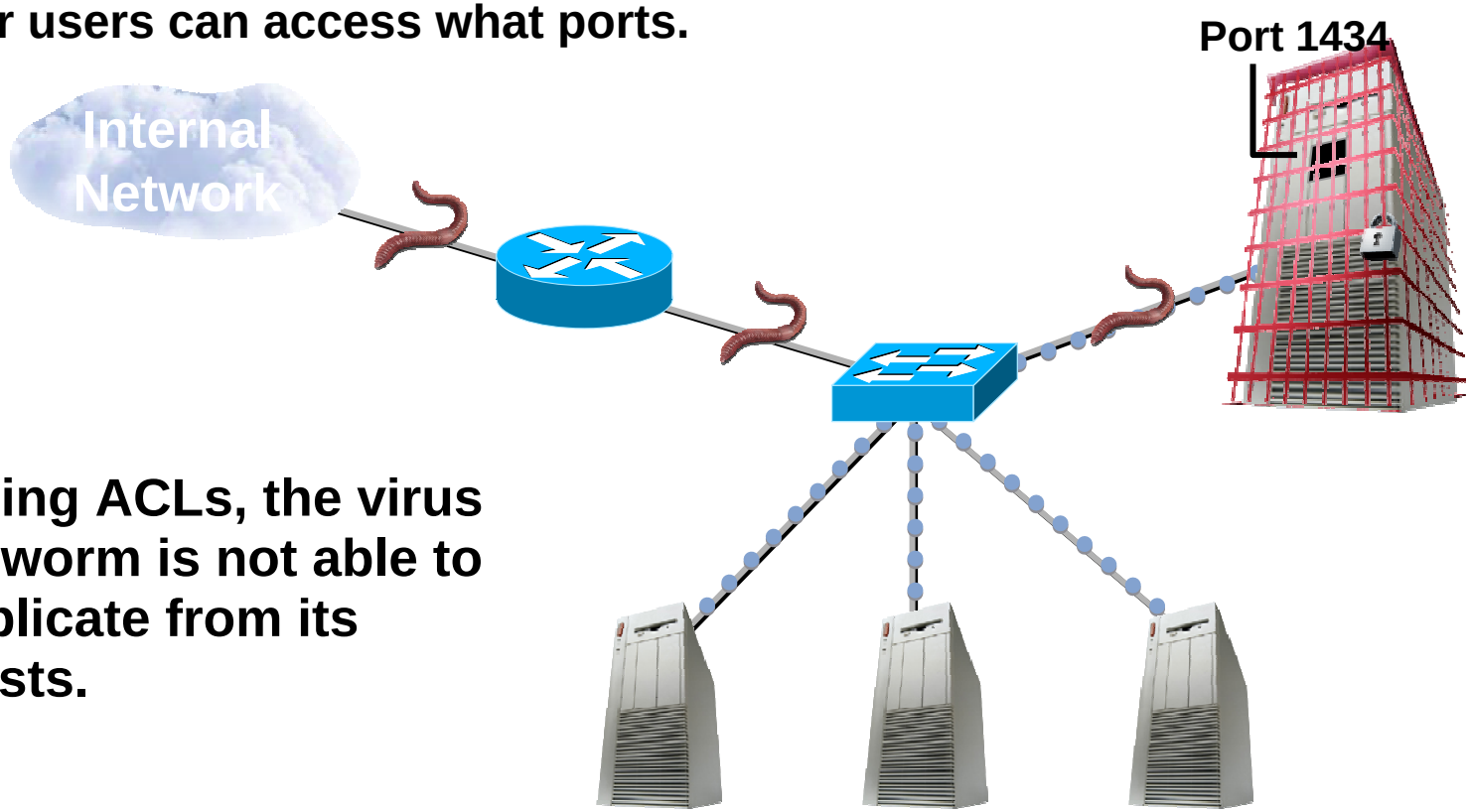
VACL - Provides granular control for limited access within a VLAN or subnet.

Time-Based ACL – ACL becomes active at certain time of the day

Protecting against Worms – 1

How It Works:

The ACL provide a mechanism to protect servers, users and applications against worms by determining what traffic streams or users can access what ports.

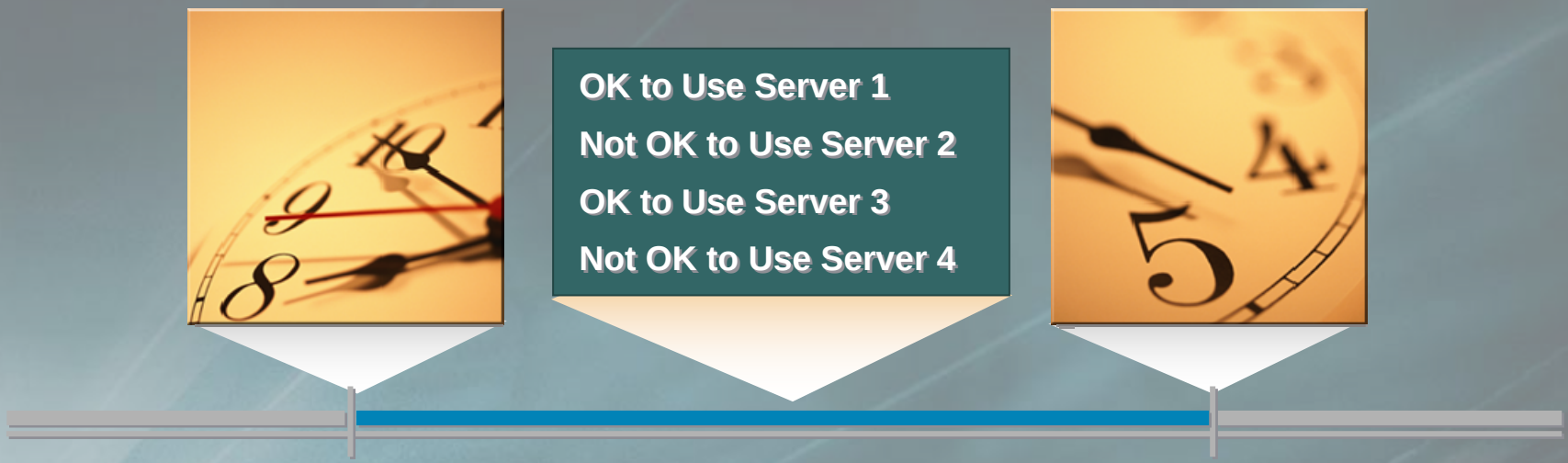


Using ACLs, the virus or worm is not able to replicate from its hosts.

Time-Based ACLs

How It Works:

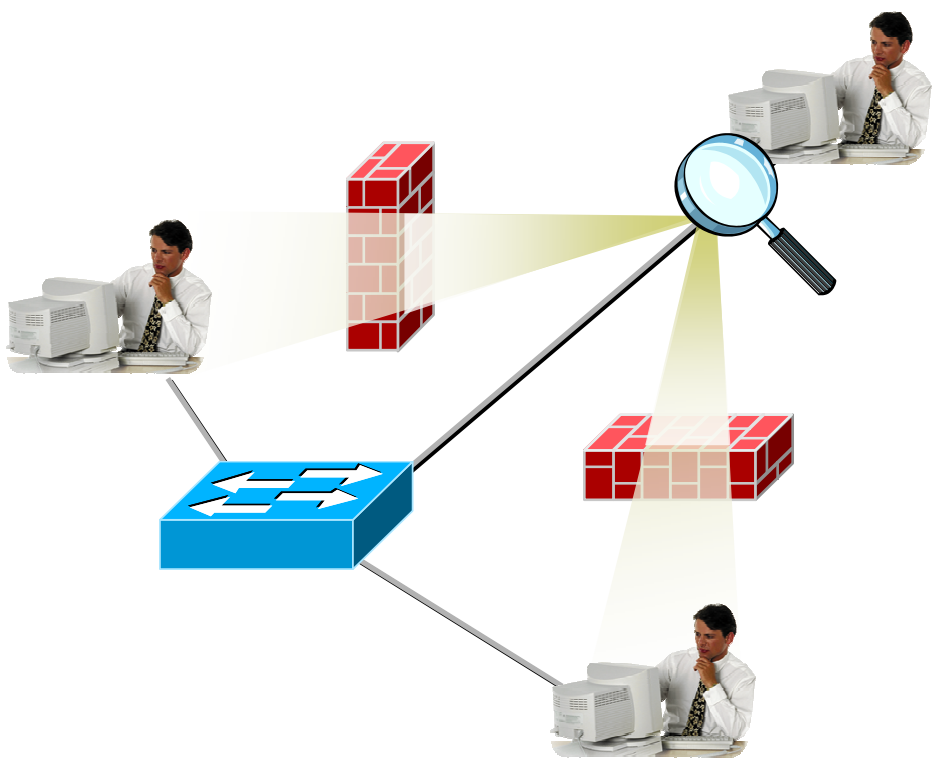
Controls the switching of data based on the time of day.



ACL goes on at 8:00 AM

ACL goes off at 5:00 PM

Keeping Neighbors Separated



Problem:

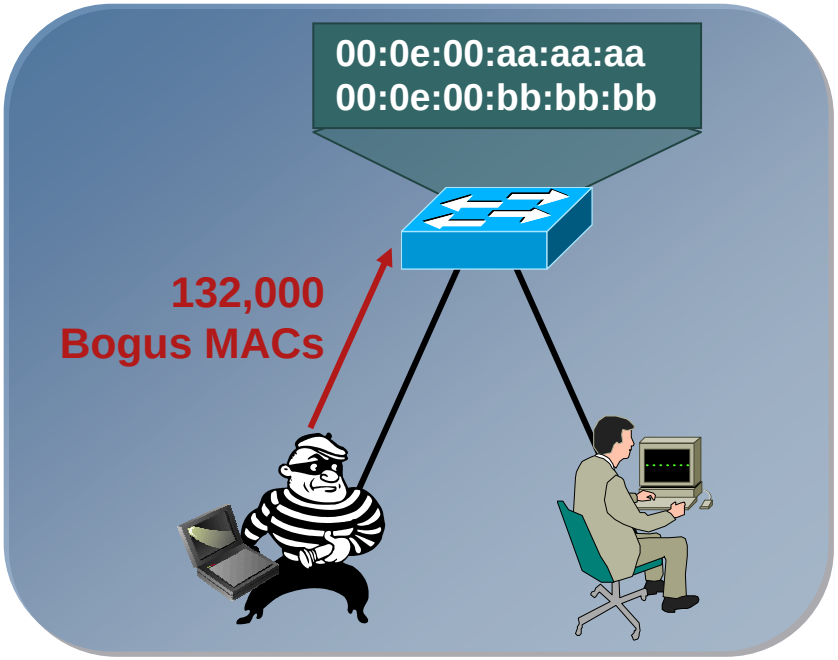
Neighbors on the same switch can view each others traffic, including logon ID and passwords. Enforcing policy on how traffic is passed between workgroups

Solution:

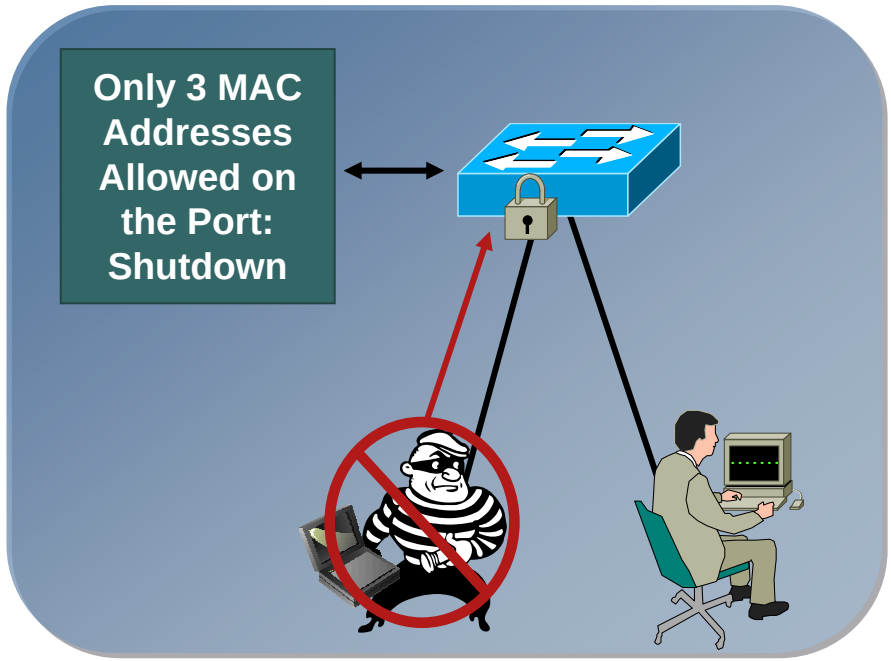
Private VLAN Edge to block Layer 2 traffic between the users in same VLAN

Raising the Bar on Surveillance Attacks

MAC Flooding Attacks



- "Script Kiddie" hacking tools enable attackers flood switch CAM Tables with bogus macs; turning the VLAN into a "hub" and eliminating privacy
- Switch CAM Table supports a limited # of Mac Addresses



- Port security limits MAC flooding attack and locks down port and sends an SNMP trap

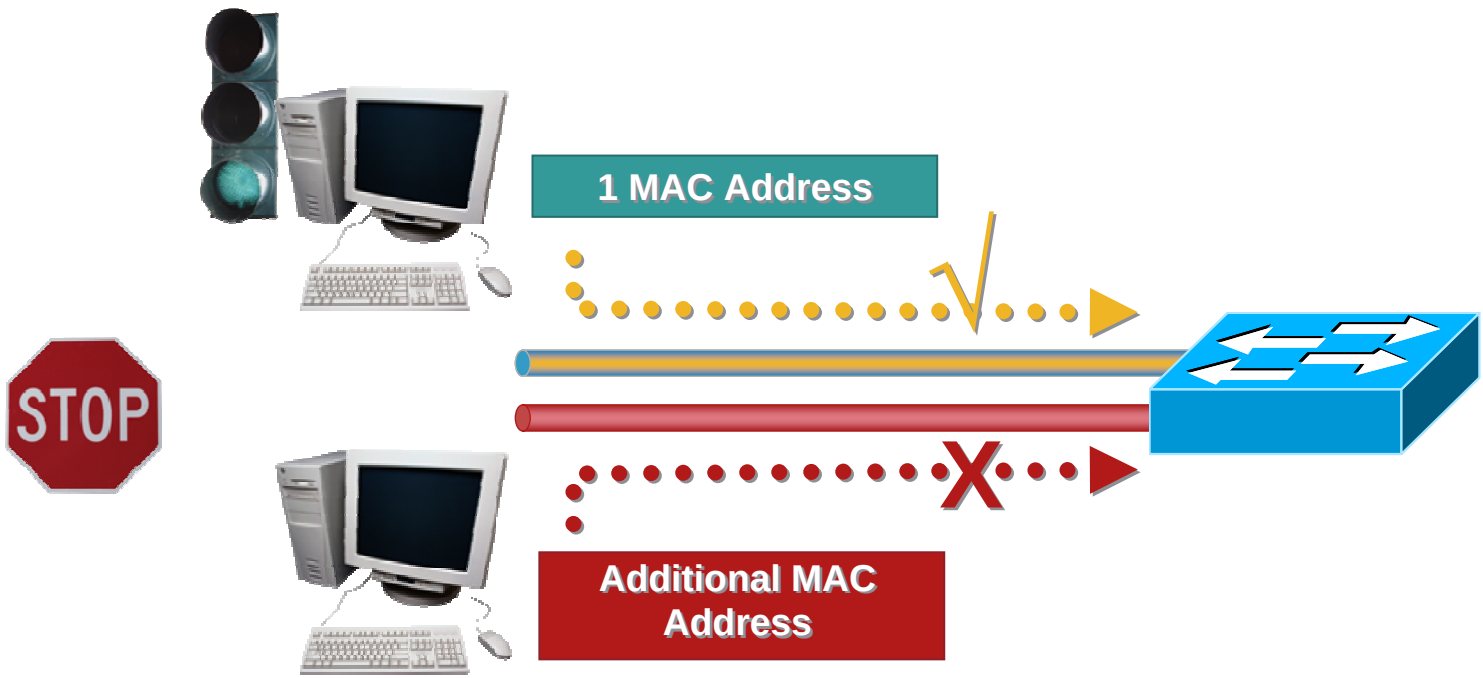
Port Security

What It Does:

Limits the number of MAC addresses that are able to connect to a switch and ensures only approved MAC addresses are able to access the switch.

Benefit:

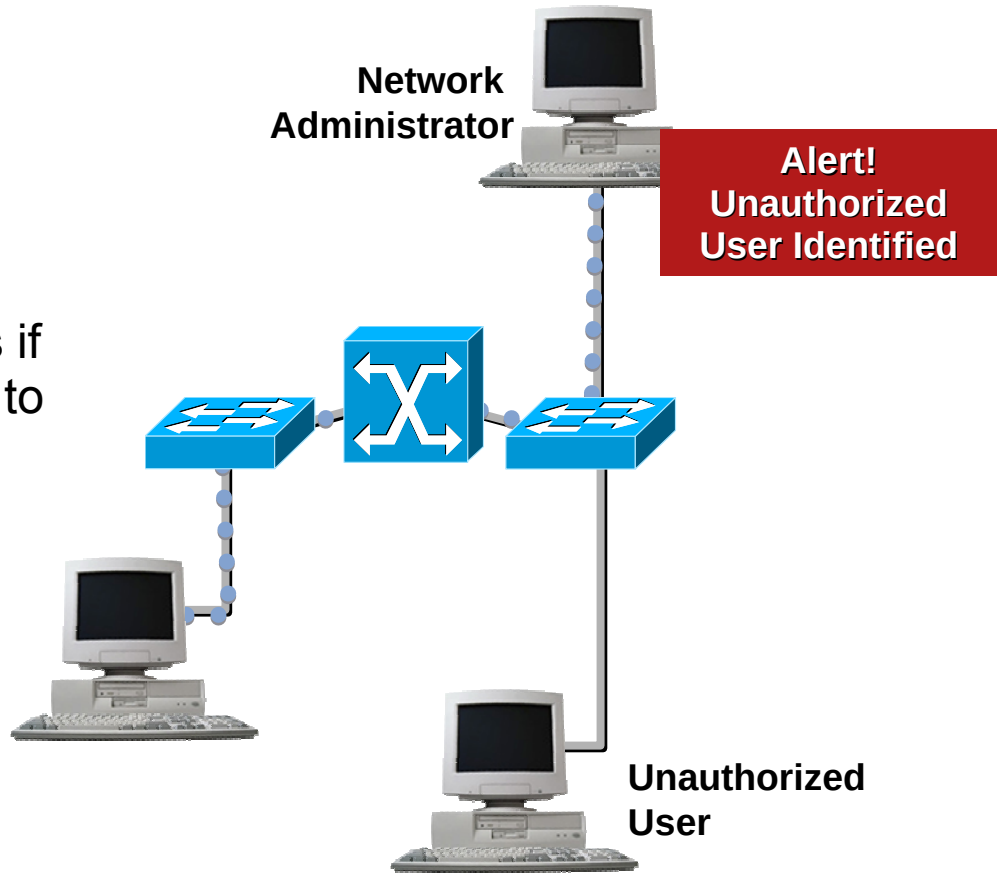
Ensures only approved users can log on to the network.



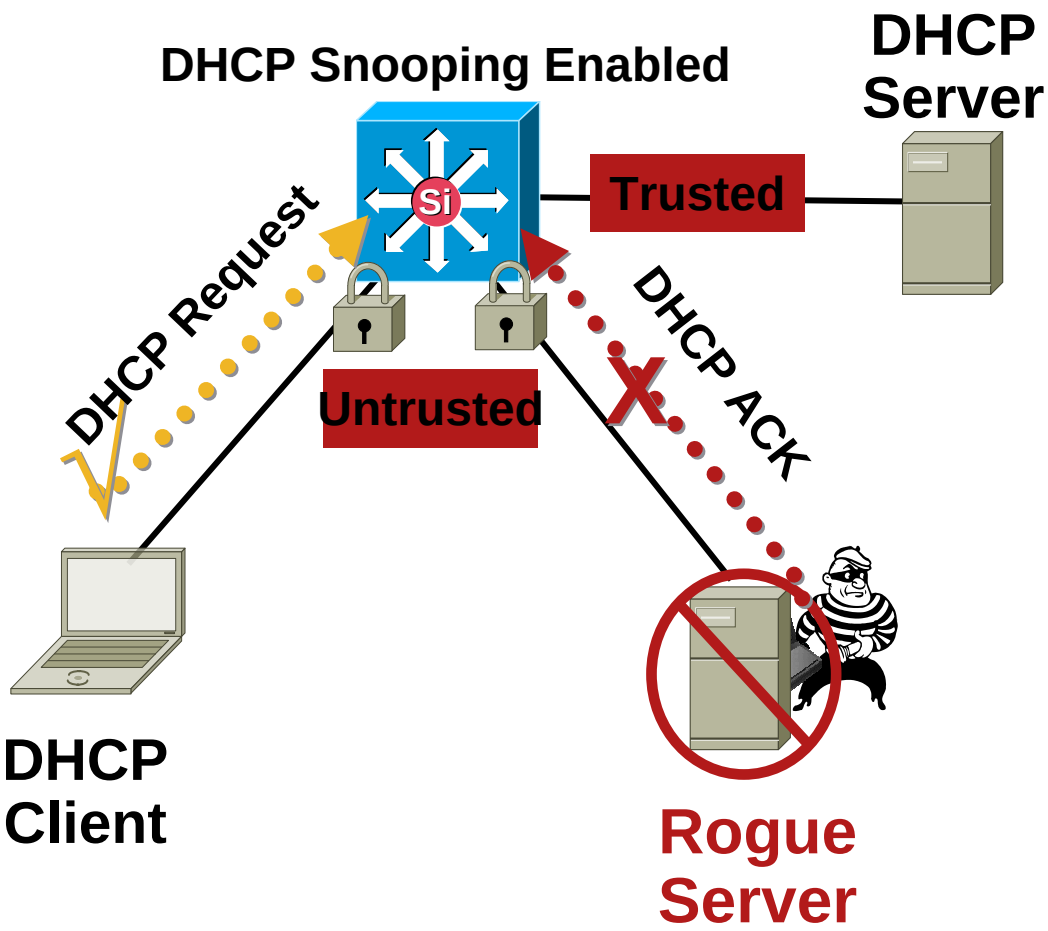
Notification for Intrusion

- MAC Address Notification

  Alerts network administrators if unauthorized users come on to the network.



DHCP Snooping



What It Does:

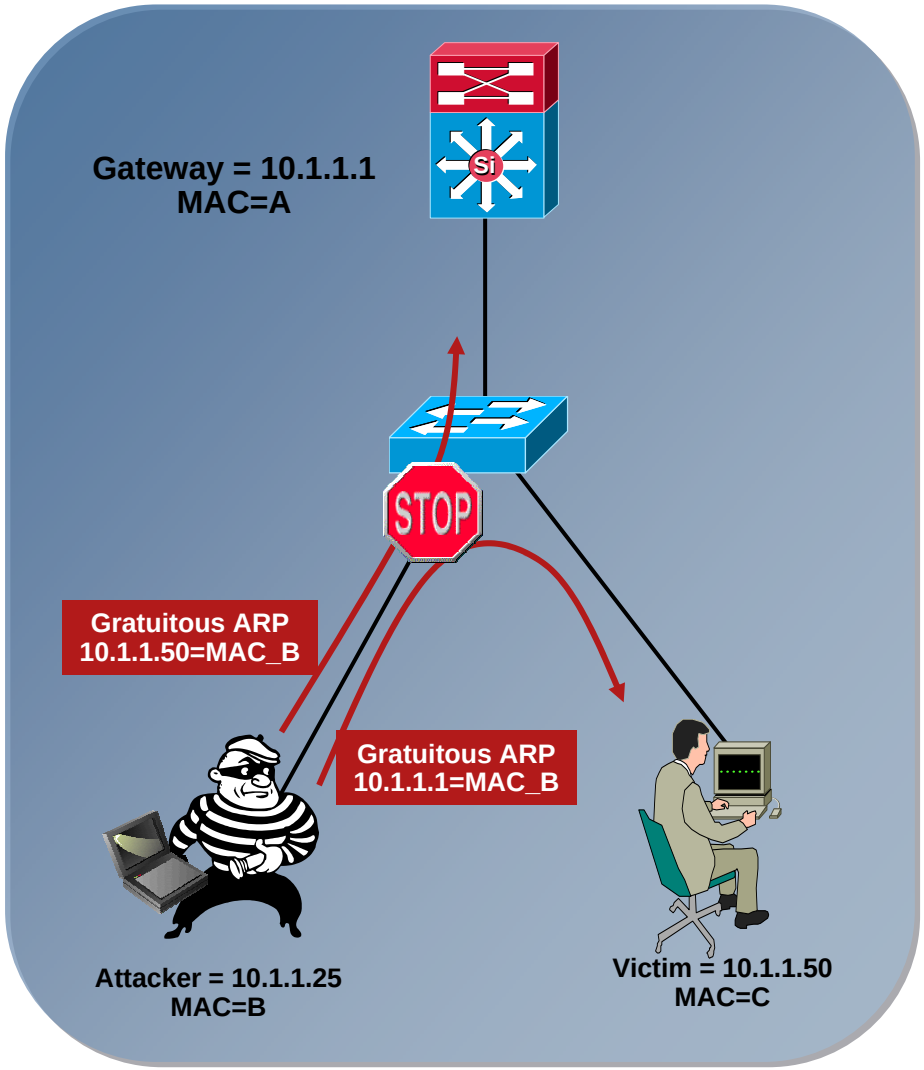
Switch forwards only DHCP requests from untrusted access ports, drops all other types of DHCP traffic. Allows only designated DHCP ports or uplink ports trusted to relay DHCP Messages

Builds a DHCP binding table containing client IP address, client MAC address, port, VLAN number

Benefit:

Eliminates rogue devices from behaving as the DHCP server

Dynamic ARP Inspection

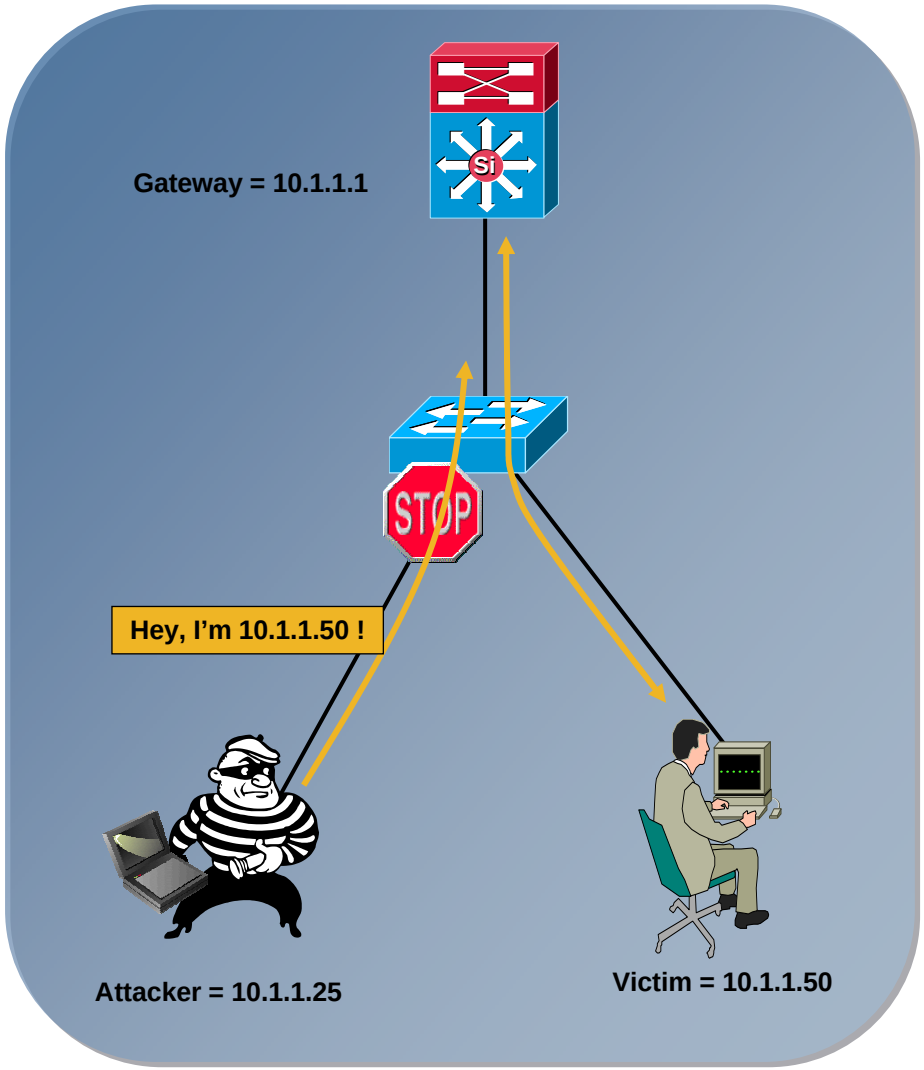


Dynamic ARP Inspection *Protects against ARP Poisoning*

- Uses the DHCP snooping binding table
- Tracks MAC to IP from DHCP transactions
- Rate-limits ARP requests from client ports; stop port scanning
- Drop BOGUS ARP's; prevents ARP poisoning/MIM attacks

IP Source Guard

Protection against Spoofed IP Addresses



IP Source Guard Protects against spoofed IP Addresses

- Uses the DHCP snooping binding table
- Tracks IP address to port associations
- Dynamically programs port ACL to drop traffic not originating from IP address assigned via DHCP

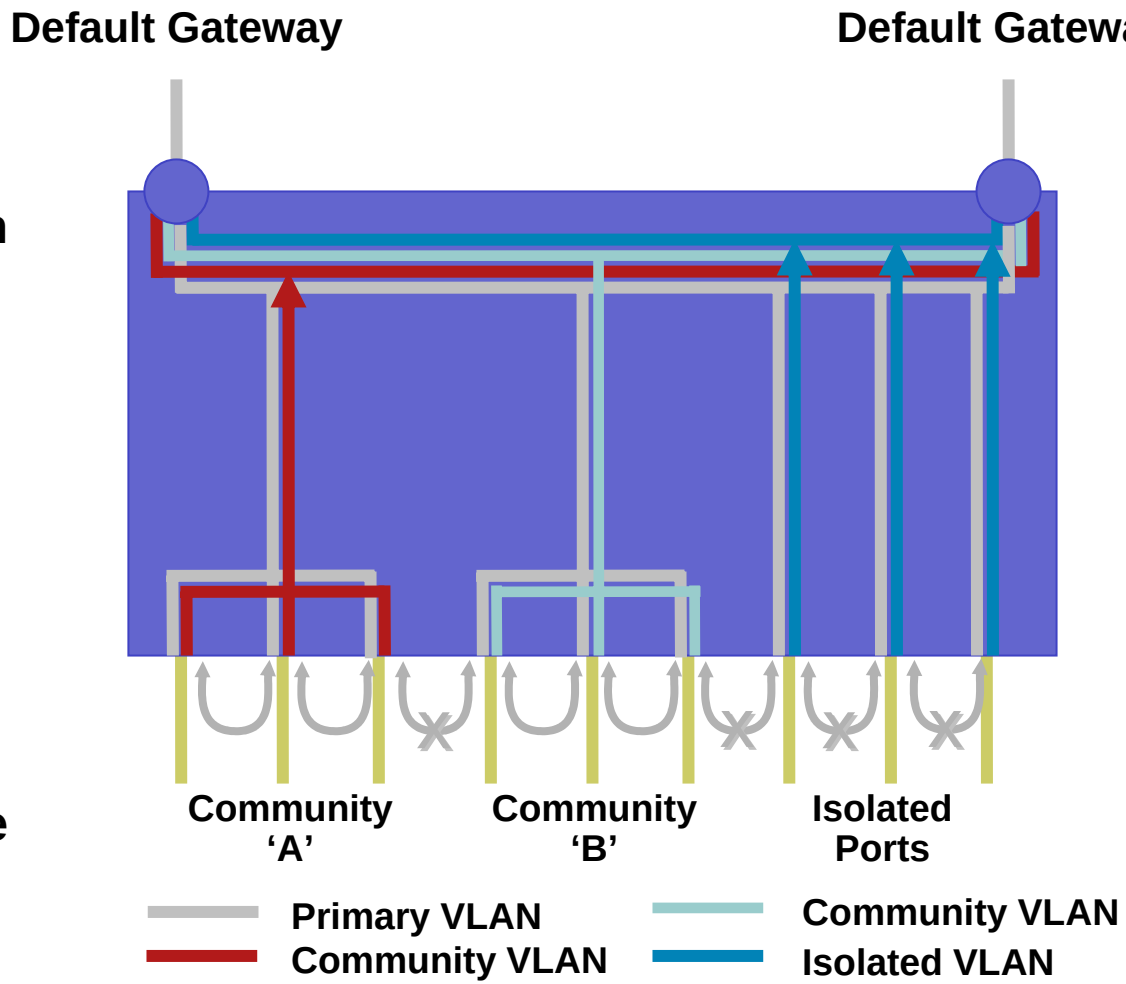
Private VLAN

How it Works:

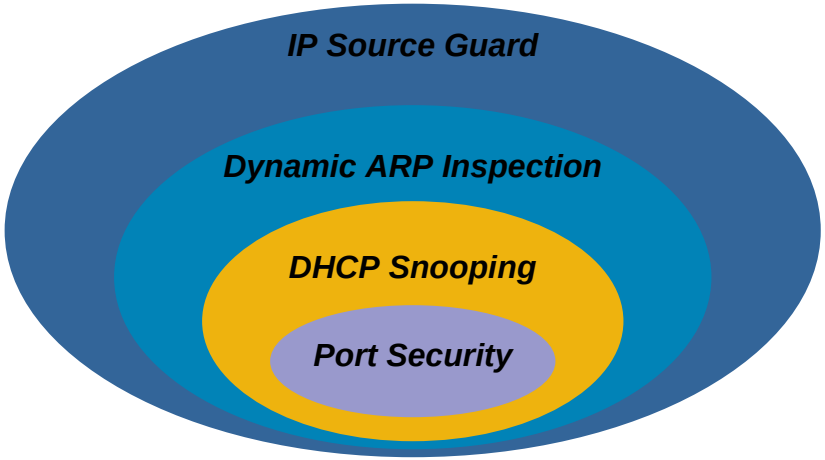
A common subnet is sub-divided into multiple private-VLANs. Hosts on given Private VLAN can only communicate with default gateway — NOT with other hosts on network.

Benefit:

Simplified mechanism of traffic management while conserving IP address space



Catalyst Integrated Security Features
Summary IOS



- Port Security prevents MAC flooding attacks
- DHCP snooping prevents client attack on the switch and server
- Dynamic ARP Inspection adds security to ARP using DHCP snooping table
- IP Source Guard adds security to IP source address using DHCP snooping table
- All features work on switchports

```
ip dhcp snooping
ip dhcp snooping vlan 2-10
ip arp inspection vlan 2-10
!
interface fa3/1
switchport port-security
switchport port-security max 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
!
Interface gigabit1/1
ip dhcp snooping trust
ip arp inspection trust
```

Cisco Security Agent: Host Based Intrusion Prevention

Endpoint + Network = Effective Collaborative Security

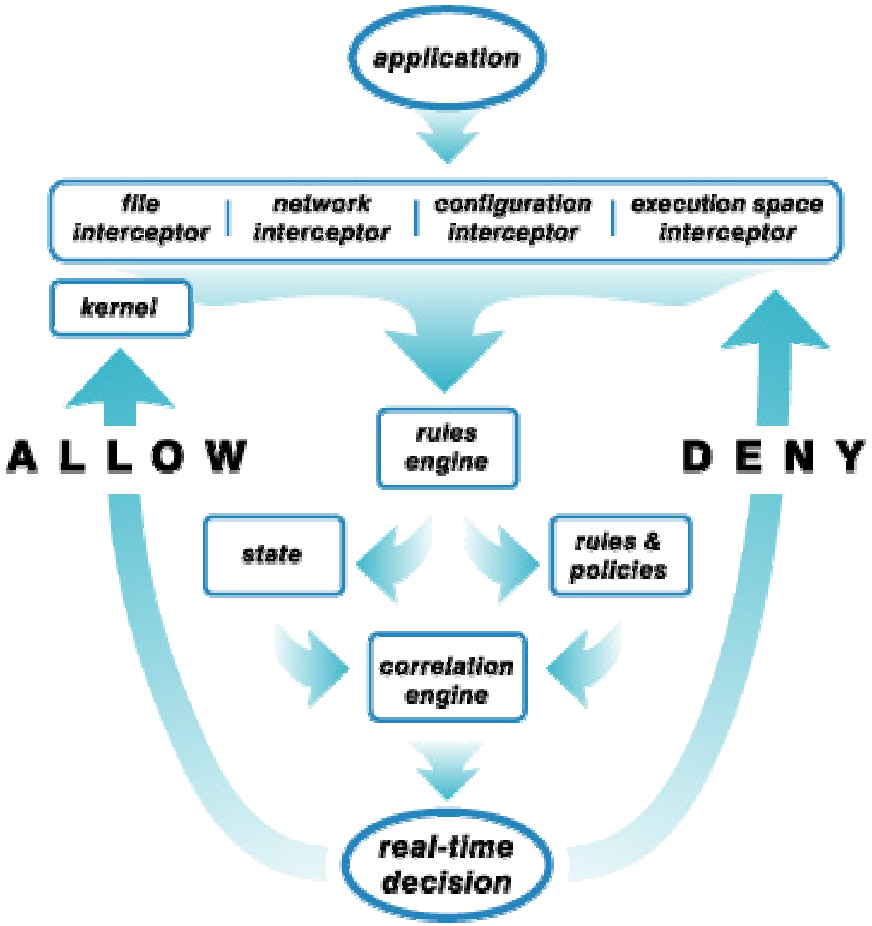
Novembre 2006

Zero-Day Protection

- Cisco defines Host-Based Intrusion Prevention as the ability to stop Zero Day malicious code without reconfiguration or update.
- CSA has effectively stopped Zero Day exploits, worms, and viruses over past 6 years:
  - 2001 – Code Red, Nimda (all 5 exploits), Pentagone (Gonner)
  - 2002 – Sircam, Debploit, SQL Snake, Bugbear,
  - 2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer
  - 2004 – MyDoom, Bagle, Sasser, JPEG browser exploit (MS04-028), RPC-DCOM exploit (MS03-039), Buffer Overflow in Workstation service (MS03-049)
  - 2005 – Internet Explorer Command Execution Vulnerability, Zotob
  - 2006 – Internet Explorer textrange vulnerability

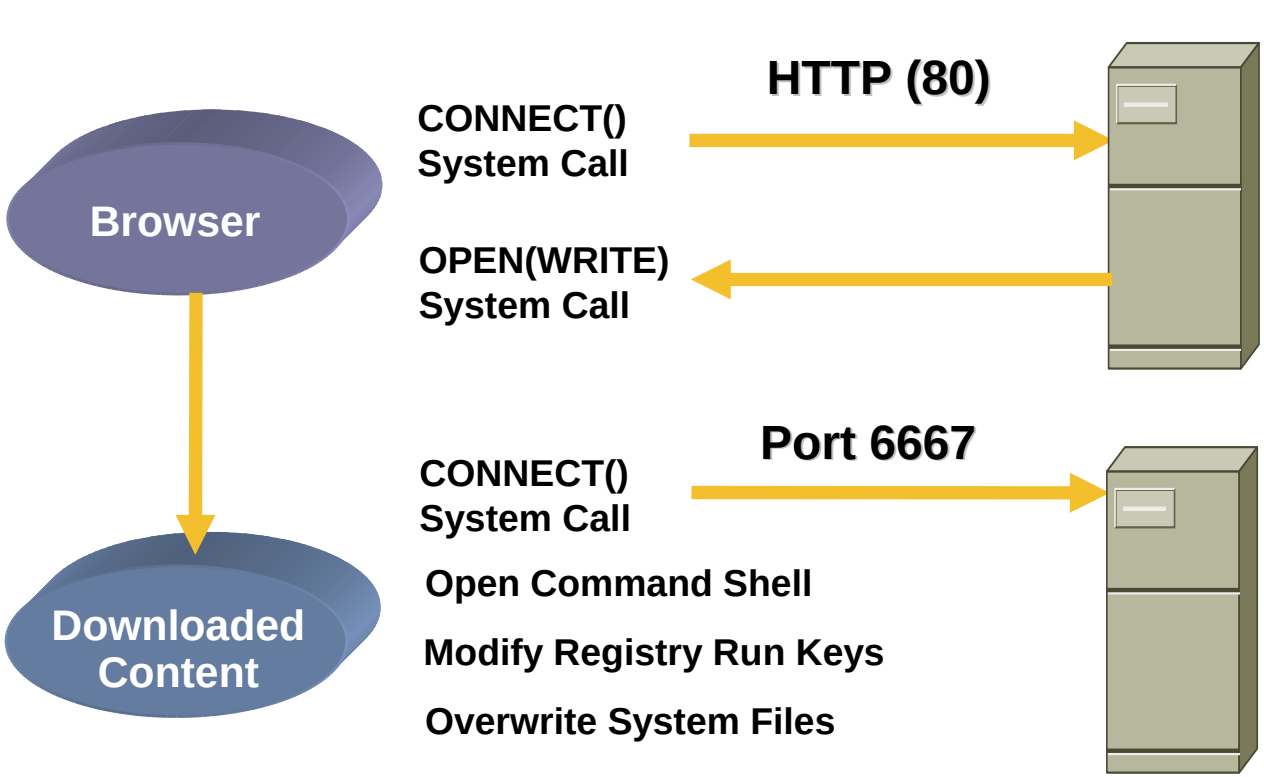
No signatures, reconfiguration or binary updates required

Intercepting Operating System Calls



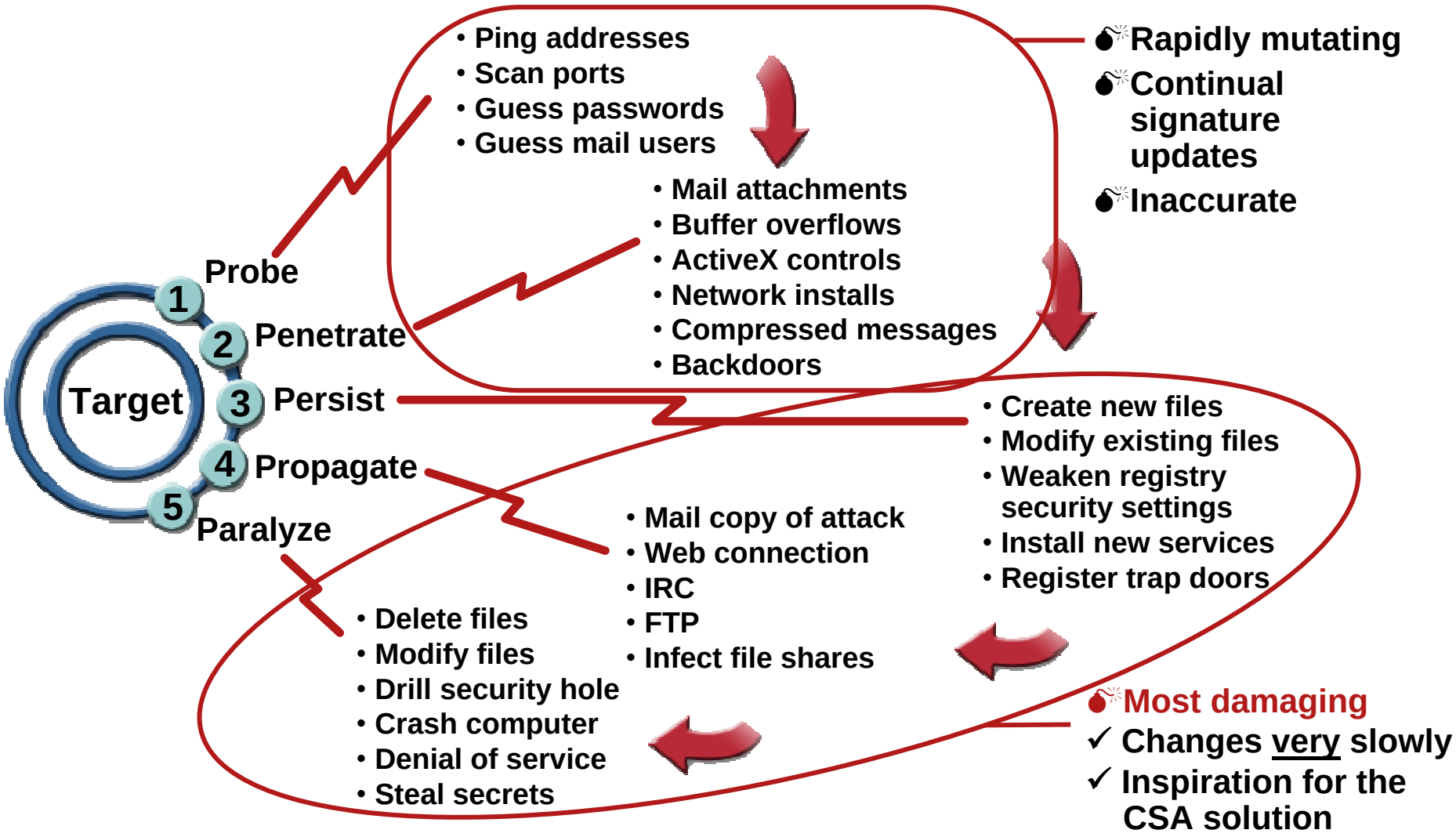
- The Cisco Security Agent intercepts application OS calls and invokes an allow/deny response
- Interceptors monitor calls for resource access:
  - File system
  - Network (inbound/outbound)
  - Registry
  - Execution (process creation, library access, executable invocation)
- "Zero Update" architecture – behavior based control means you don't need a new signature to stop the next attack

Correlation

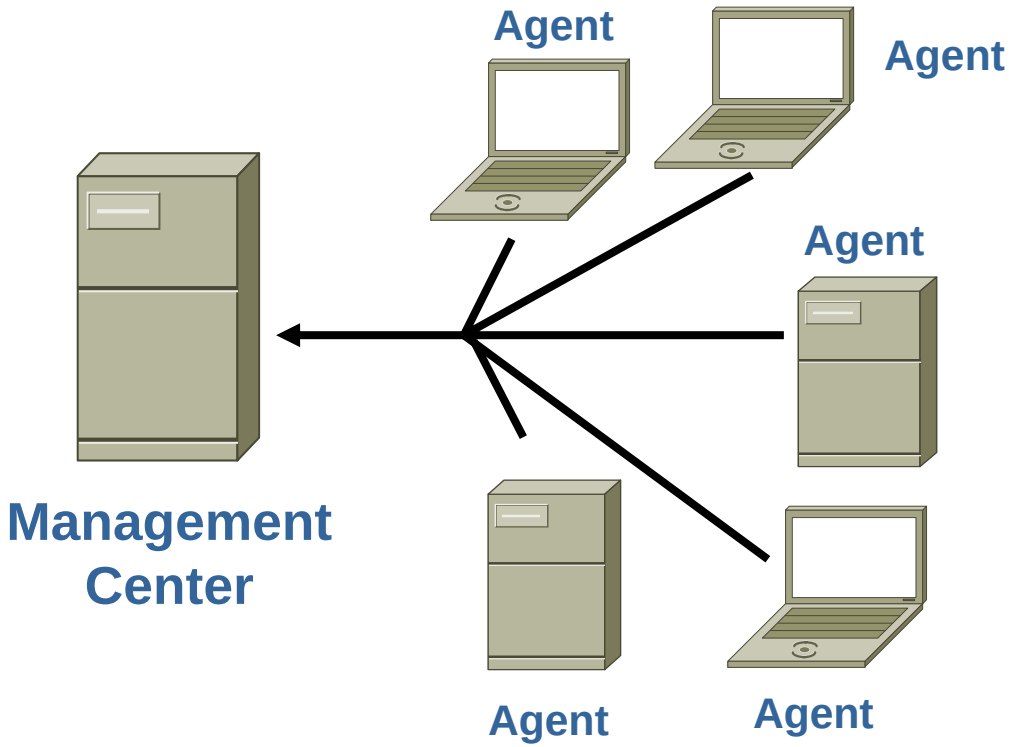


Malicious behavior is most accurately identified in context. Cisco Security Agent correlation does this automatically – no configuration required.

Malicious Behavior



Global Correlation



Cisco Security Agent offers unique agent and management level correlation

Correlation on Agent
- Higher accuracy
- Fewer "False Positive" events

Correlation on Manager
- Higher accuracy
- Fewer "False Negative" events
- Stops attack before it reaches targets

Example: Distributed "Ping Scans", Network Worm propagation

CSA Policy Control

- Some types of behavior are not malicious, but are undesired because they violate Acceptable Use policy
  - Music sharing via Peer-to-Peer (p2p) applications
  - Instant messaging using non-corporate IM servers
  - Protecting sensitive organizational data
  - Configuration lockdown during end of year reporting period
  - Which devices cannot be used (USB memory, multimedia devices)
  - Use of unauthorized applications, or unauthorized versions of apps
- CSA policy control modules include
  - Data Theft Prevention policy
  - Instant Messenger Control policy
  - Music Download Prevention policy
  - Network Lockdown policy

Provide user feedback via pop-up query and audit to demonstrate compliance

Quality of Service (QoS) as a Solution

QoS Benefits

DURING DISASTER

Mission critical data still gets through

Latency sensitive applications will not be affected

IN GENERAL

Cost savings – especially on WAN links

QoS Challenges

Trust boundary generally ends at the access switch

Lengthy configuration process based on addresses and ports

Many applications don't have QoS functionality

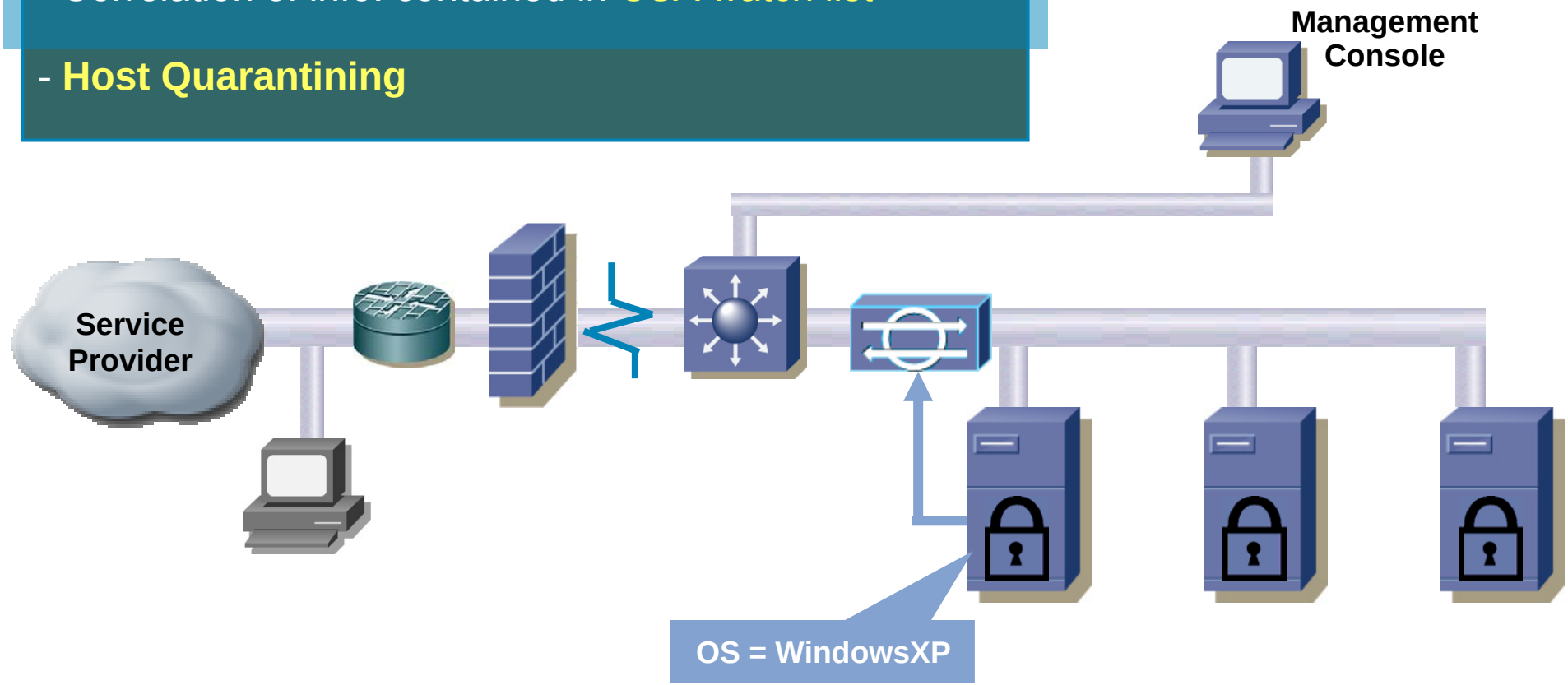
Cheaters can skew service delivery

Entirety of QoS responsibility rests with network ops

CSA + IPS Collaboration
with Cisco Network IPS Version 6.0

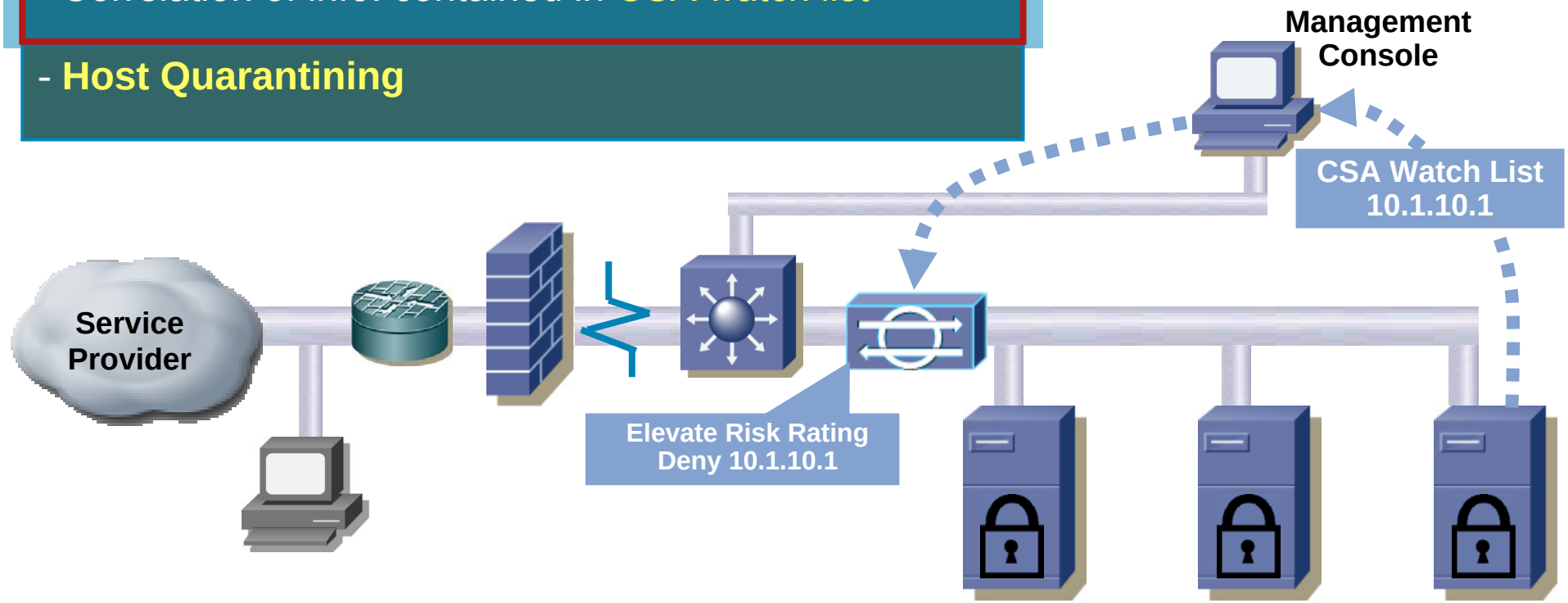
- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list

- **Host Quarantining**



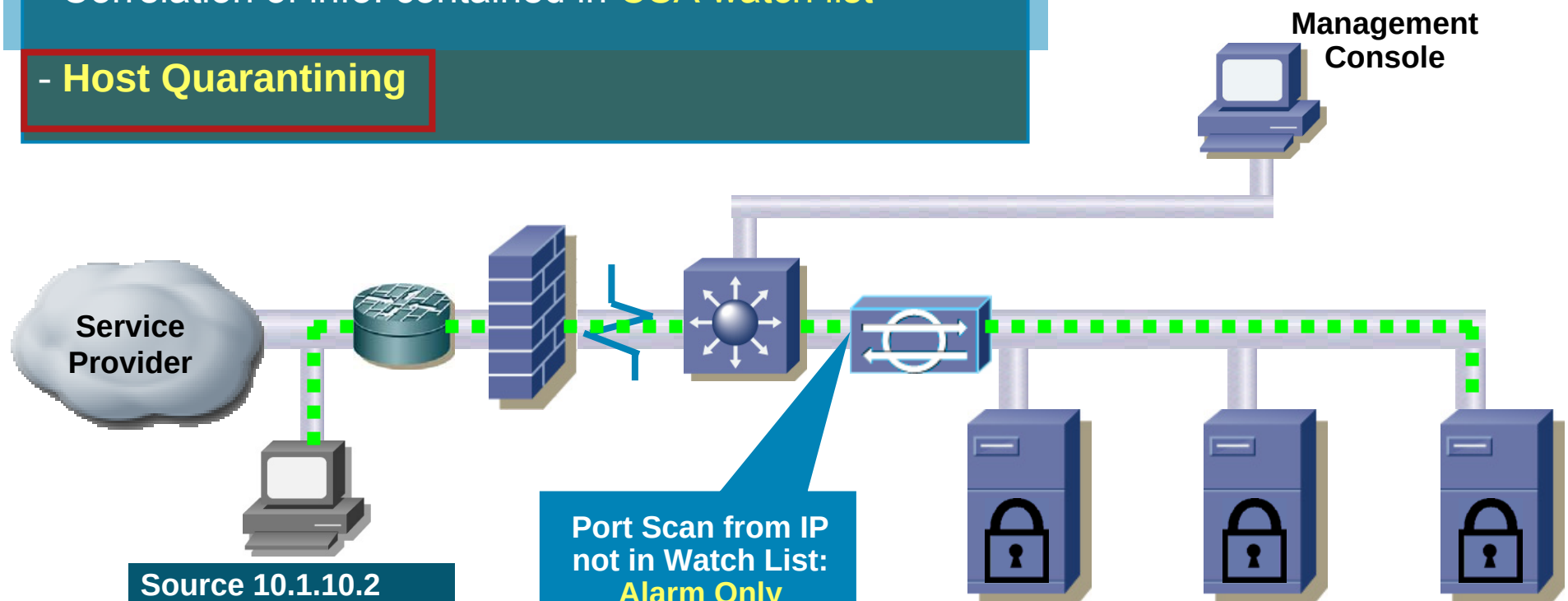
CSA + IPS Collaboration
with Cisco Network IPS Version 6.0

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- **Host Quarantining**



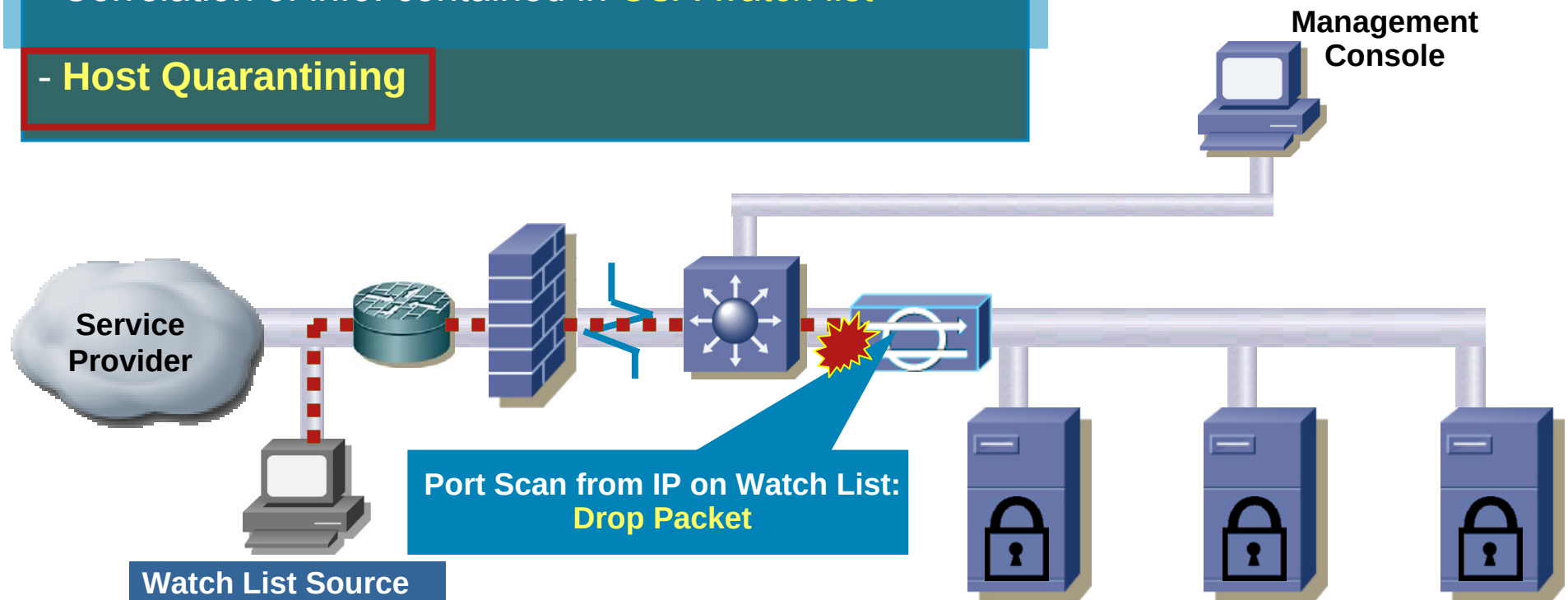
CSA + IPS Collaboration
with Cisco Network IPS Version 6.0

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- **Host Quarantining**



CSA + IPS Collaboration
with Cisco Network IPS Version 6.0

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- **Host Quarantining**



How does Cisco Security Agent investigation work?

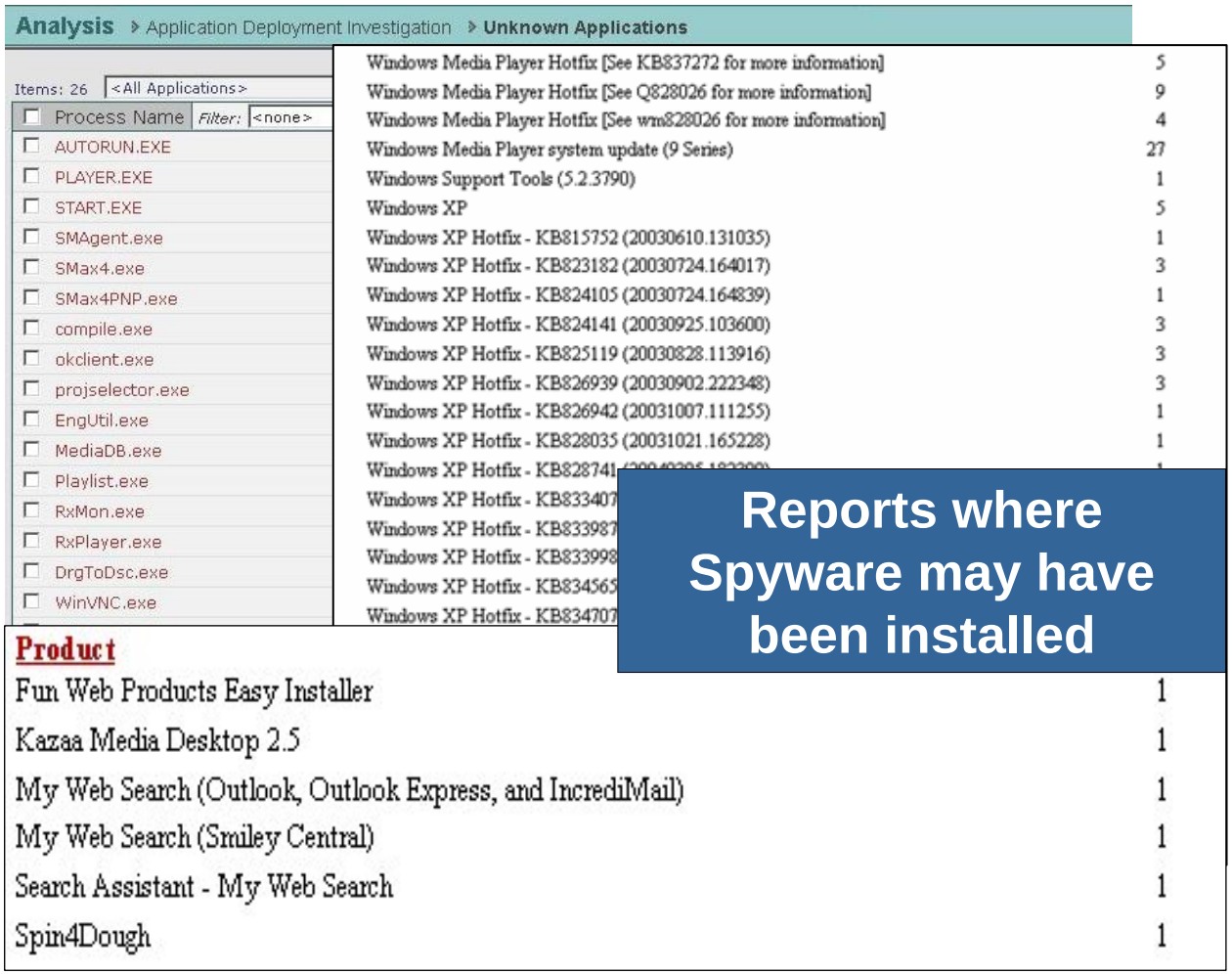
What do I have?

What do I use?

Is it at risk or malicious?

How do I control it?

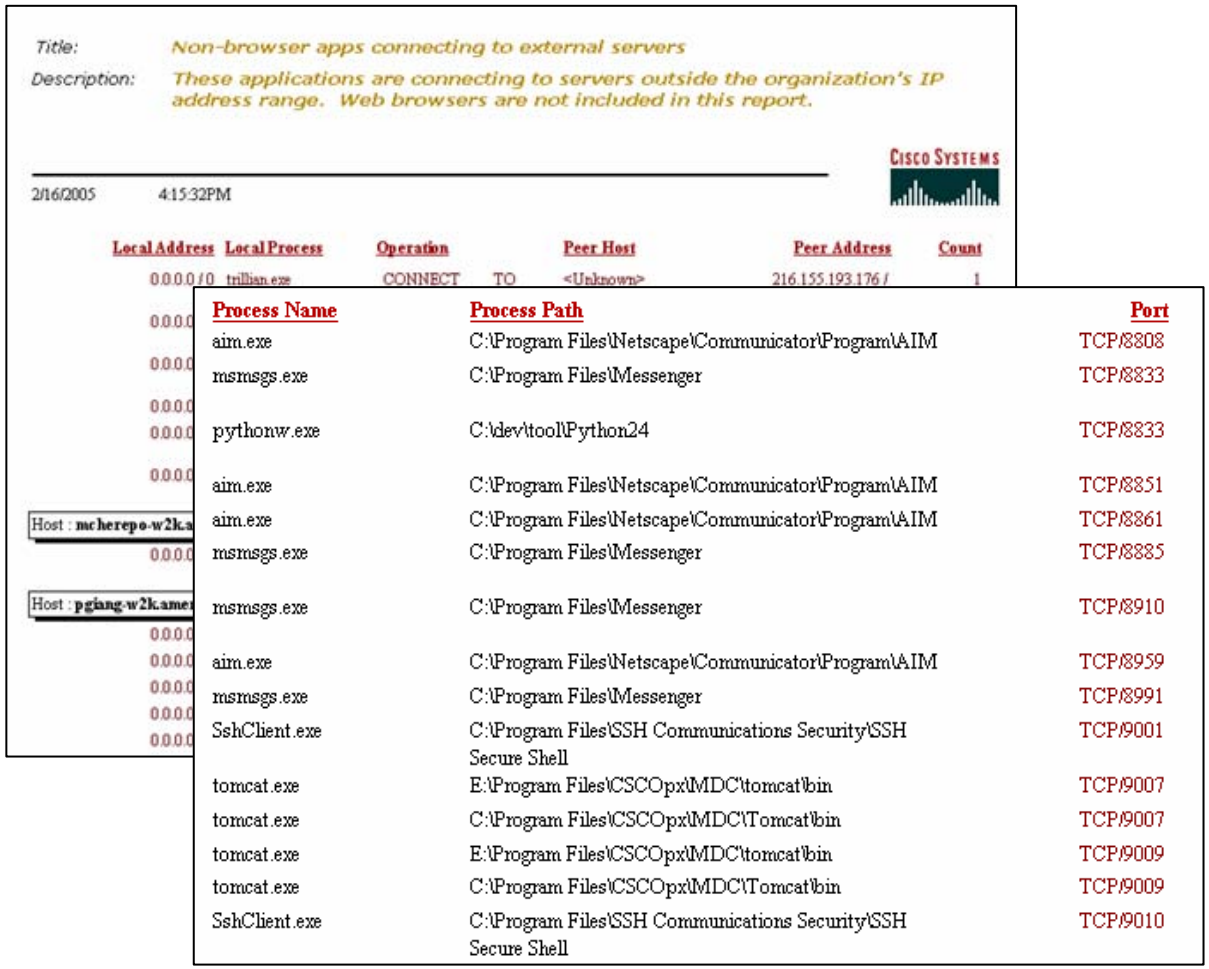
What Do I Have?



Which known and unknown apps are installed?

Which hotfixes are installed?

What Do I Use?



Title: Non-browser apps connecting to external servers

Description: These applications are connecting to servers outside the organization's IP address range. Web browsers are not included in this report.

Cisco Systems

2/16/2005 4:15:32PM

Local Address	Local Process	Operation		Peer Host	Peer Address	Count
0.0.0.0 / 0	trillian.exe	CONNECT	TO	<Unknown>	216.155.193.176 /	1

Host : mcherepo-w2k.a

Host : pgiang-w2k.amer

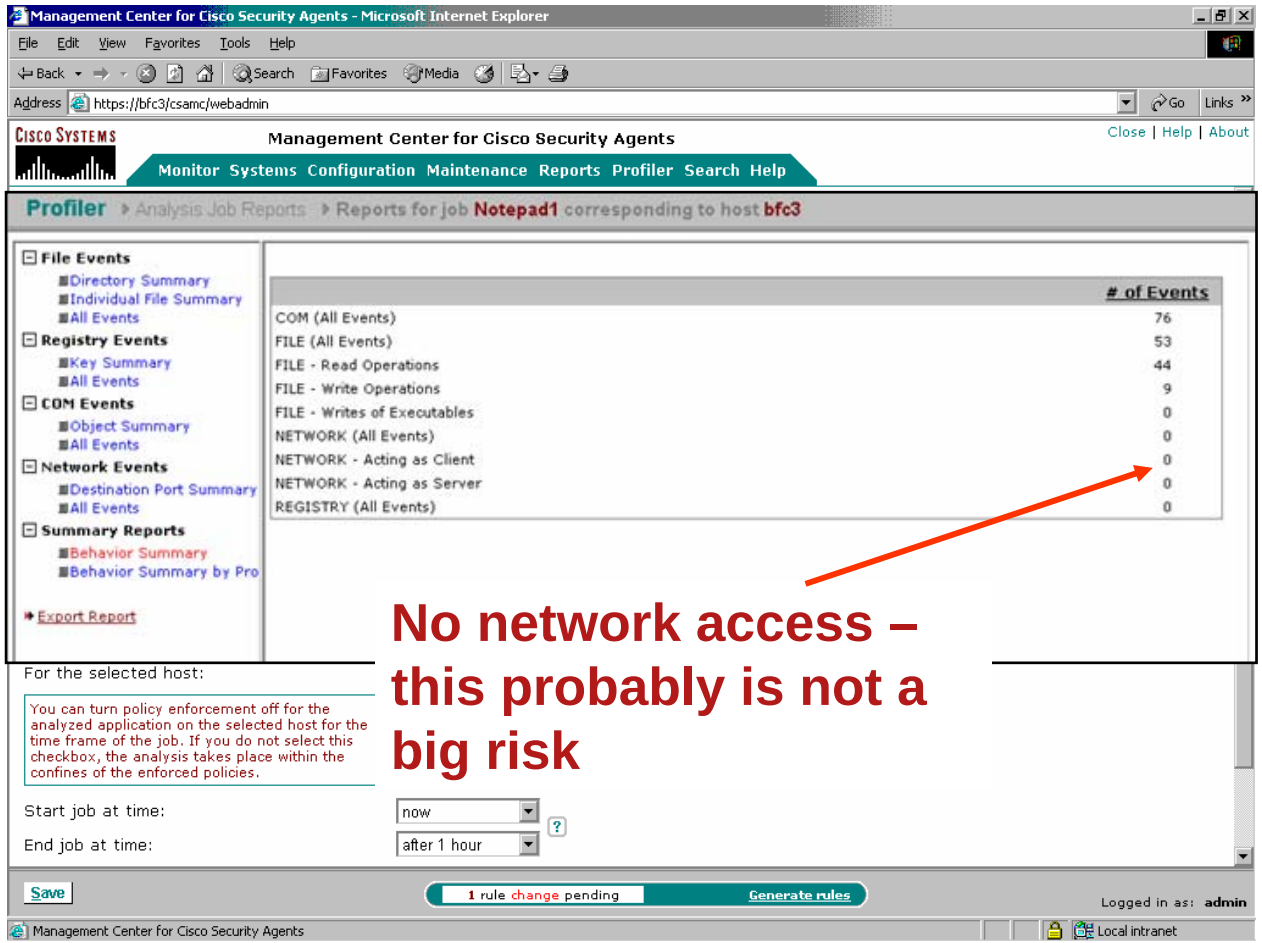
Process Name	Process Path	Port
aim.exe	C:\Program Files\Netscape\Communicator\Program\AIM	TCP/8808
msmsgs.exe	C:\Program Files\Messenger	TCP/8833
pythonw.exe	C:\dev\tool\Python24	TCP/8833
aim.exe	C:\Program Files\Netscape\Communicator\Program\AIM	TCP/8851
aim.exe	C:\Program Files\Netscape\Communicator\Program\AIM	TCP/8861
msmsgs.exe	C:\Program Files\Messenger	TCP/8885
msmsgs.exe	C:\Program Files\Messenger	TCP/8910
aim.exe	C:\Program Files\Netscape\Communicator\Program\AIM	TCP/8959
msmsgs.exe	C:\Program Files\Messenger	TCP/8991
SshClient.exe	C:\Program Files\SSH Communications Security\SSH Secure Shell	TCP/9001
tomcat.exe	E:\Program Files\CSCOpx\MDC\tomcat\bin	TCP/9007
tomcat.exe	C:\Program Files\CSCOpx\MDC\Tomcat\bin	TCP/9007
tomcat.exe	E:\Program Files\CSCOpx\MDC\tomcat\bin	TCP/9009
tomcat.exe	C:\Program Files\CSCOpx\MDC\Tomcat\bin	TCP/9009
SshClient.exe	C:\Program Files\SSH Communications Security\SSH Secure Shell	TCP/9010

Not all installed apps are actually used

CSA can track which ones are and how they communicate

Reports unnecessary apps (servers that listen on a port but don't accept connections)

Is it at Risk?



CSA monitors all file, Registry, COM, and Network behavior

Unknown apps can be easily investigated, even when the agent is remote

Suspicious apps can be verified to be malicious or safe, from central location

How Do I Control It?

- Cisco Security Agent policy fine grained control:
  - Disallow execution of the app
  - Allow execution, but block the bad behavior
  - Use Query messages to let the user know that what they are doing is being audited
- Cisco Security Agent offers a *behavior-based feedback loop* so that you can actively understand and control what is happening on end points

Feedback Loop helps control identified behavior and refine default policies, without visiting the endpoint

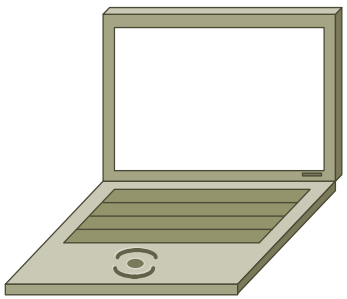
Trusted Boot

BIOS Update

Boot to non-primary disk

No CSA running

NAC Posture: QUARANTINE



Boot to primary disk

CSA State: INSECURE BOOT

NAC Posture: REMEDIATE

NAC

Dynamic Policy Change

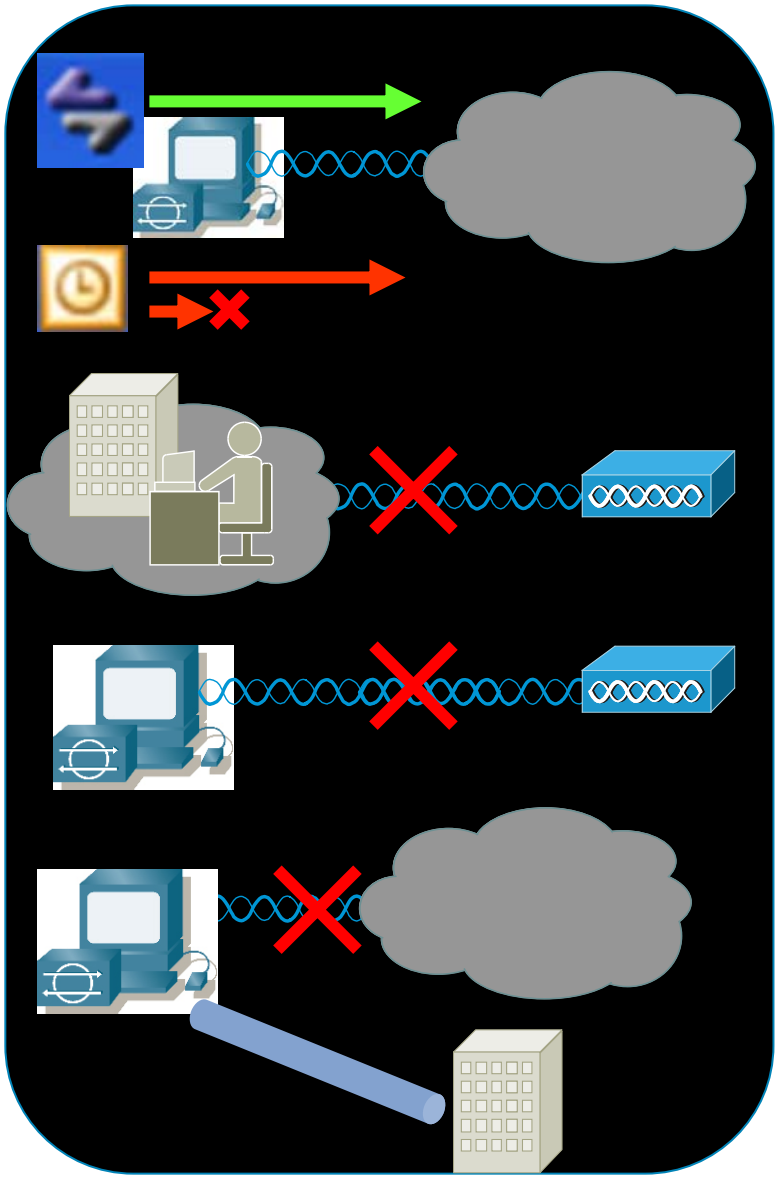
Boot History

Latest boot events (max 10):

#	Time	Boot Type	Event Source
2	11/8/2005 5:06:03 PM	Safe mode	Cisco Security Agent
	Safe mode boots since previous Cisco Security Agent run: 1		
1	11/8/2005 4:58:00 PM	Removable drive	Cisco Security Agent
	2 other insecure boots recorded since previous Cisco Security Agent run. Type: **Removable drive**.		

View all boot events generated by IBM-F177AE44A35

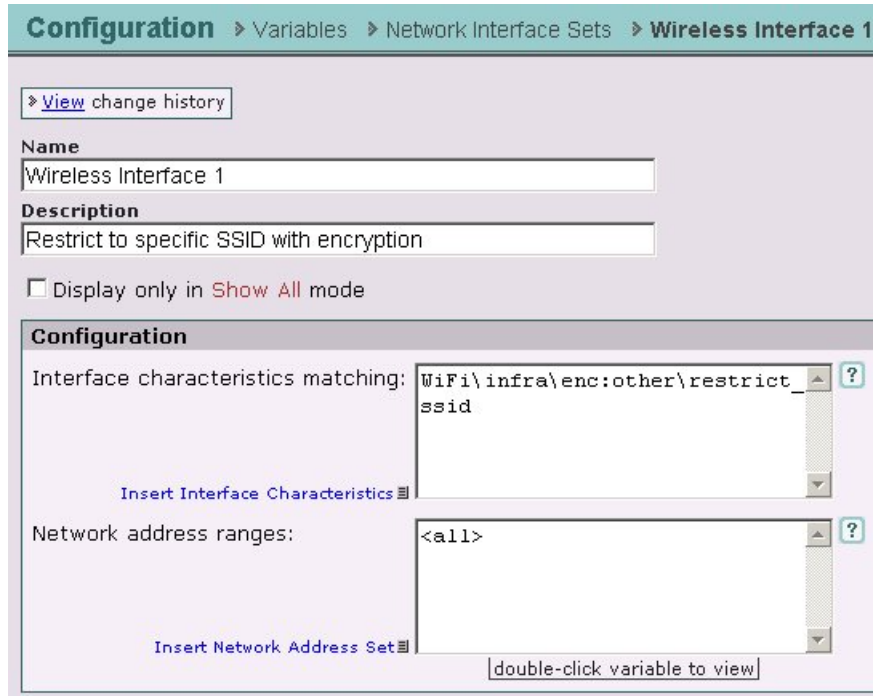
CSA 5.2 - Wireless Control

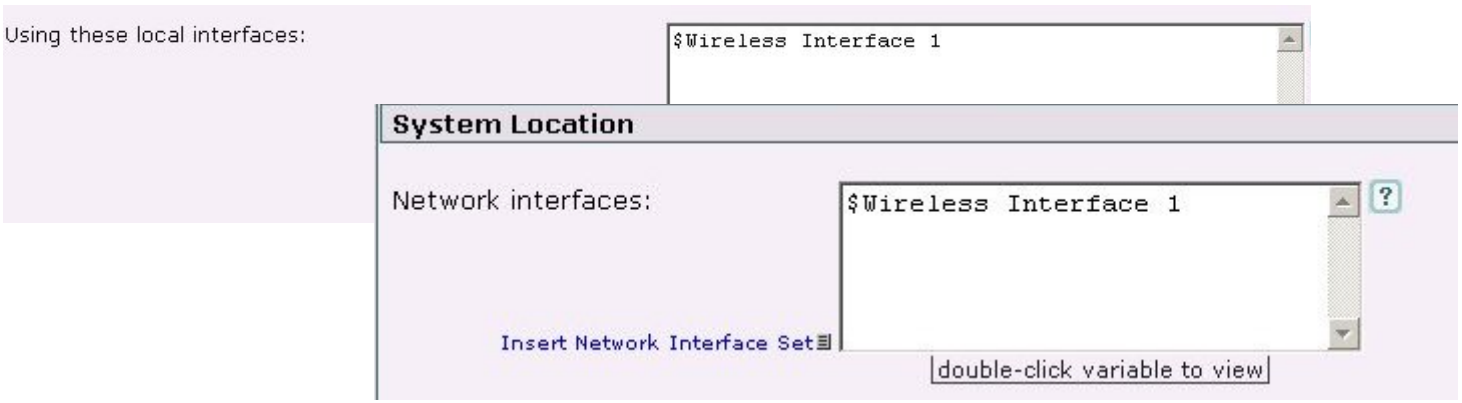


- Per-application QoS Prioritization
- Restrict wireless communication when wired NIC is active
- Connection restrictions - certain SSIDs, encryption, ad-hoc
- Require VPN connection when out of the office

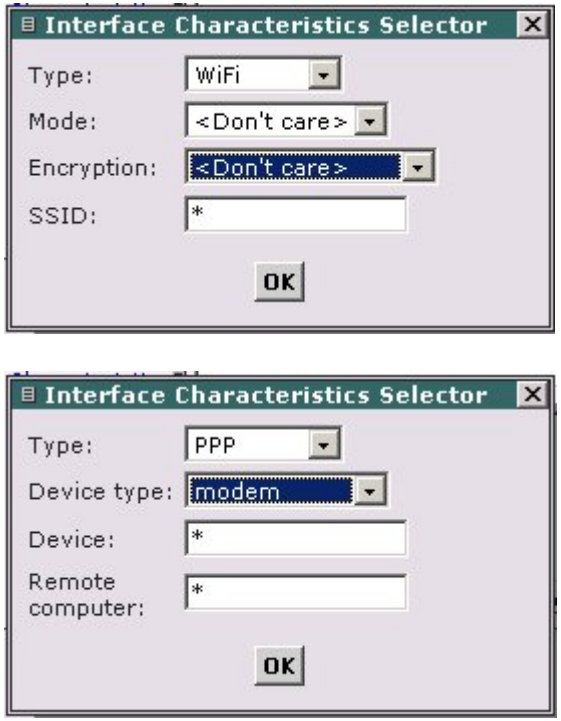
Wireless Controls

- Variable based on interface properties and other strings
- Implemented as both NACL option and system state





Additional Wireless Benefits

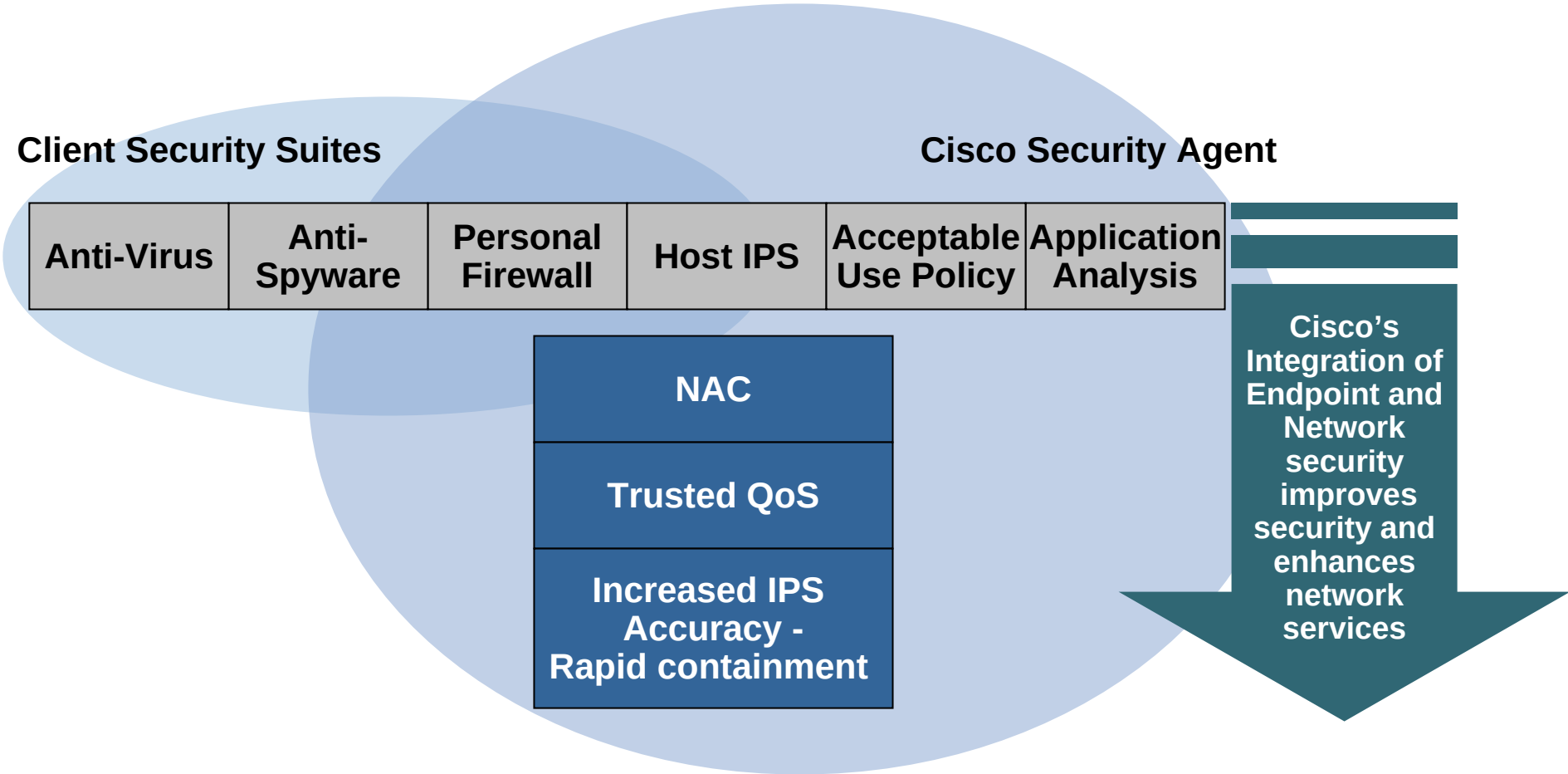


- Trunked NICs may show up as multiple virtual NICs
  - Separation of Voice and Data VLAN at the endpoint
- Broadband cards can be restricted using PPP

Information The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 445 from 192.168.45.131 using interface Wired\AMD PCNET Family PCI Ethernet Adapter. The specified action was taken to set Host Address as Untrusted host (locally and globally).

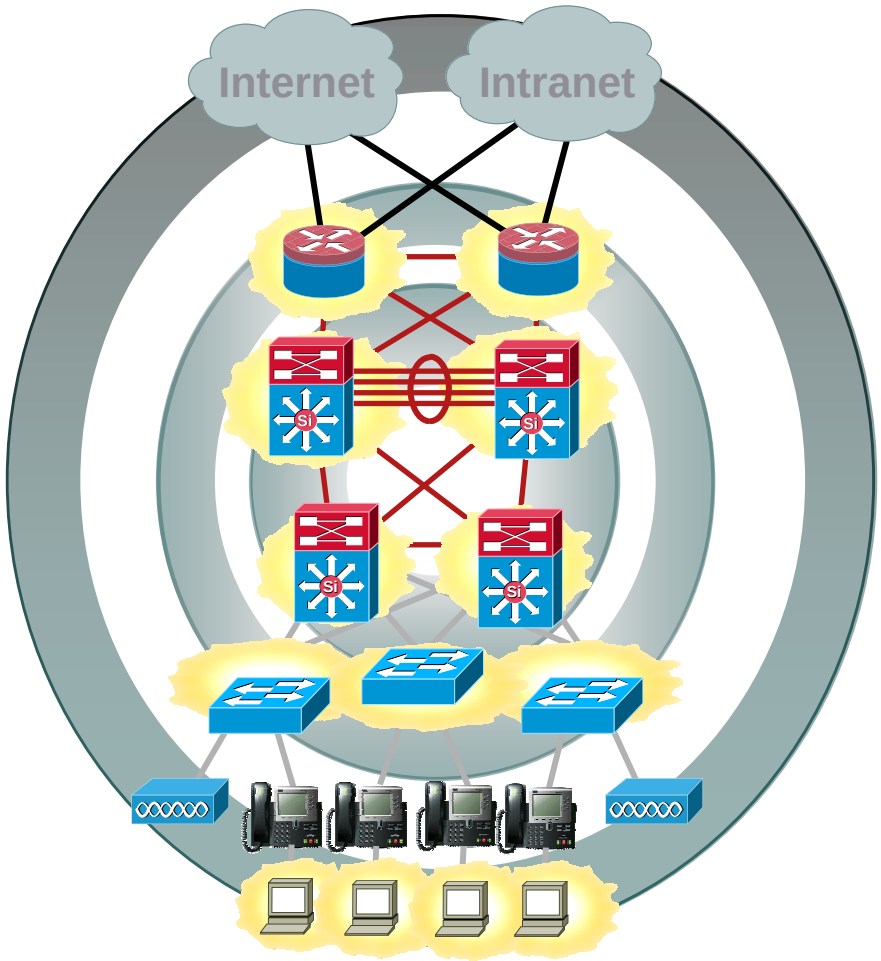
Details | Rule 51 | Wizard | Find Similar

Endpoint Security Landscape



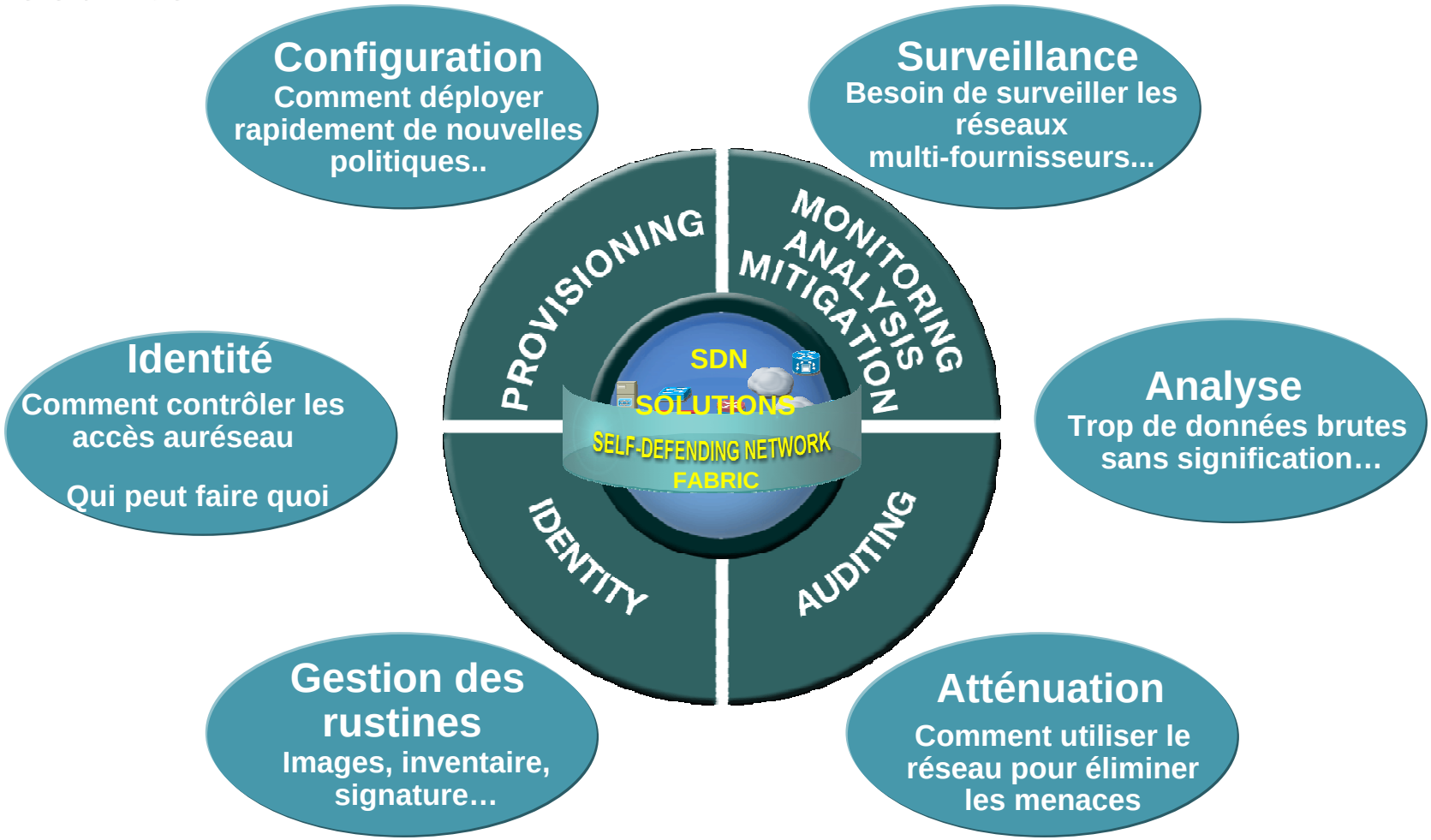
Programme

- Authentification
  - Qui peut accéder le réseau
  - L'impact de la téléphonie
  - 802.1x, les visiteurs, Web Base . Authentification
- La conformité des postes au moment de la connexion
  - Sur le LAN, en VPN, etc...
- Les bonnes pratiques pour le contrôle des usagers connectés au réseau
  - Fonctions de sécurité présentent dans les commutateurs Cisco
  - QoS déployée?
  - Cisco Securité Agent (CSA)
- La surveillance et la configuration du réseau



Gestion Unifiée de Sécurité Cisco

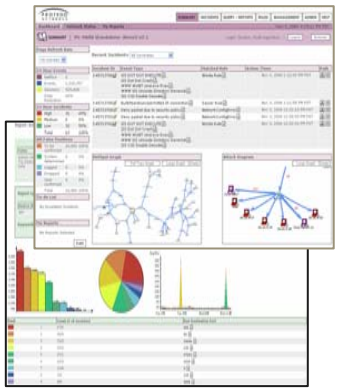
Administration et Mise en Force des Politiques de Sécurité



Réseau à capacité d'autodéfense Cisco (SDN)

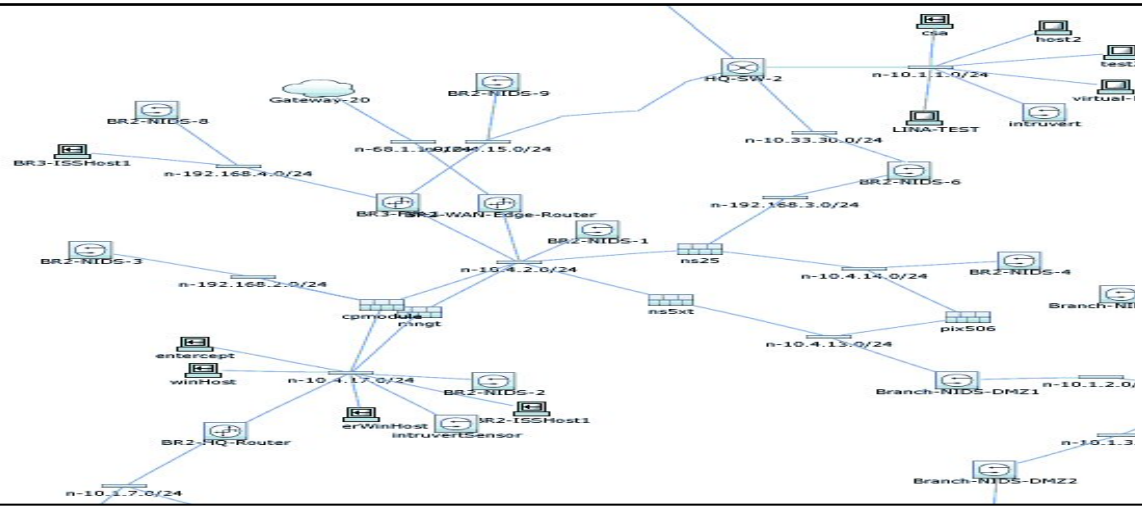
Self Defending Network

MARS



Security Manager

ACS



- Firewalls
- Proxies
- Anti-Virus
- Network IDS/IPS
- Host IDS/IPS
- Intelligent Router/Switch

Cisco Security Manager
Vue d'ensemble

Gestion des politiques

Approvisionnement des politiques de façon centrale pour pare-feu, VPN et IPS

Très extensible

Fonctions d'héritage de politique permet d'avoir des politiques uniformes sur l'ensemble de l'entreprise

Puissantes options de regroupement des dispositifs

Grande facilité d'utilisation

Gestion des politiques visuellement sur les tables ou la topologie

Aide Jumpstart : un outil d'apprentissage animé approfondi

Vues de gestion souples

- **basées sur les politiques**
- **basées sur les dispositifs**
- **basées sur la carte**
- **basées sur VPN**

Gestion des pare-feu

Configuration des politiques pour ASA, Cisco® PIX® Firewall, FWSM et le logiciel Cisco IOS®

Une seule table de règles pour toutes les plates-formes

Analyse intelligente des politiques

Modification sophistiquée de la table des règles

Compression du nombre de règles d'accès requis

Gestion VPN

Configuration de l'assistant VPN site à site, hub et spoke, et VPN entièrement maillé avec quelques clics de la souris

Configuration d'accès à distance VPN, DMVPN et dispositifs Easy VPN

Gestion IPS

Mises à jour automatiques des détecteurs IPS

Prise en charge de Outbreak Prevention Services

Configuration de Cisco Security Manager

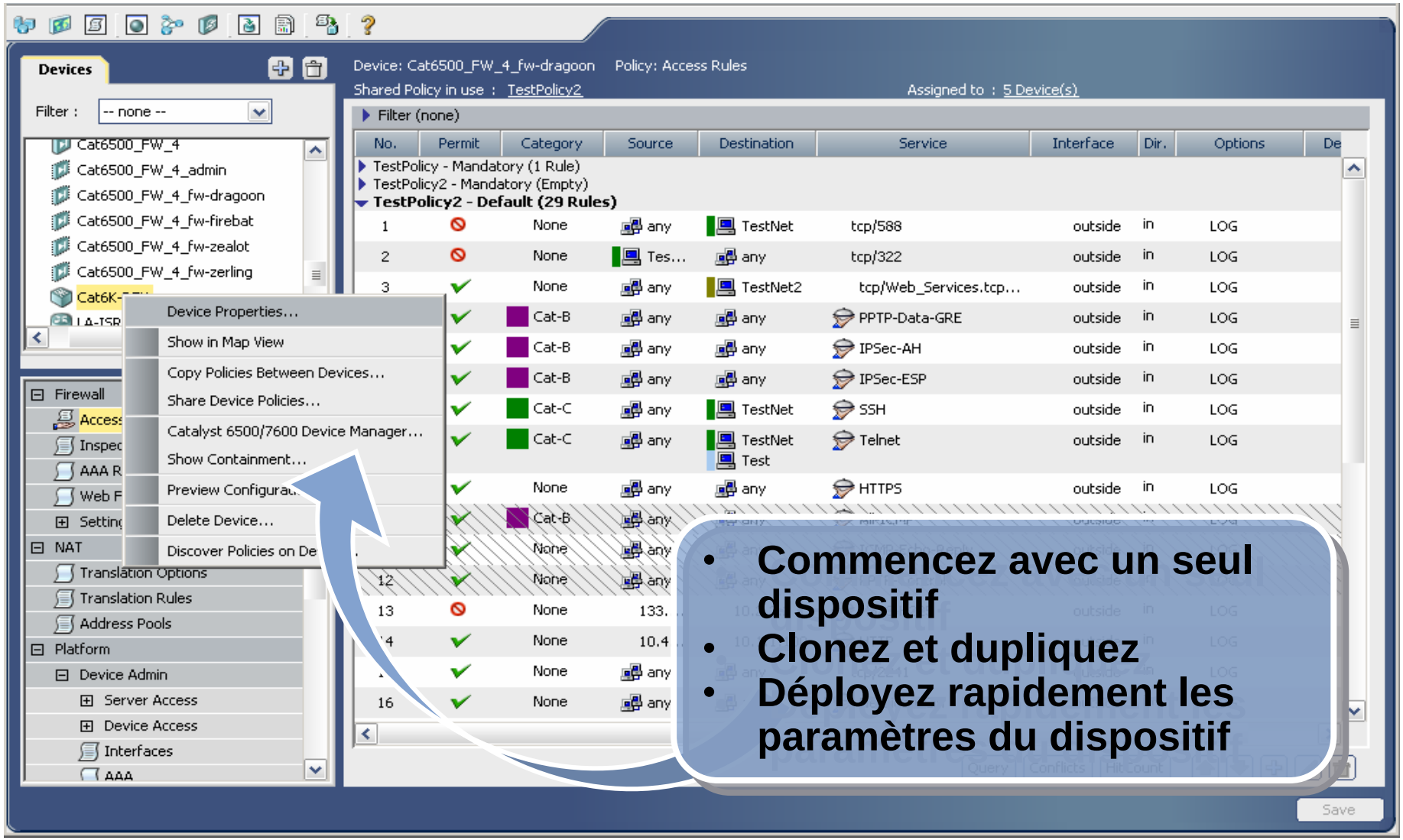
- **L'accent est mis sur la gestion de la configuration des politiques de sécurité du réseau**
- La facilité d'utilisation est essentielle
  - Procure de multiples vues pour réponde aux besoins d'exploitation
  - Offre une interface utilisateur convivial et agréable visuellement
  - Procure des assistants pour réduire la complexité
  - Offre des outils évolués pour l'utilisateur sophistiqué
- Principaux concepts de différenciation
  - Partage et héritage des politiques
  - Renforcement des politiques basées sur les domaines
  - Prise en charge des décisions du flux des travaux pour les opérations de sécurité et opérations de réseau
  - Contrôle des accès basés sur les rôles pour des opérations extensibles
  - Déploiement réparti à grande échelle

Cisco Security Manager

« Une solution conviviale et souple »

- Système frontal à fonctions enrichies
- Différentes vues pour différentes préférences de gestion
  - Dispositif
  - Topologie
  - Politique
- Formule centralisée pour la création et la personnalisation VPN
- Gestion unifiée de services

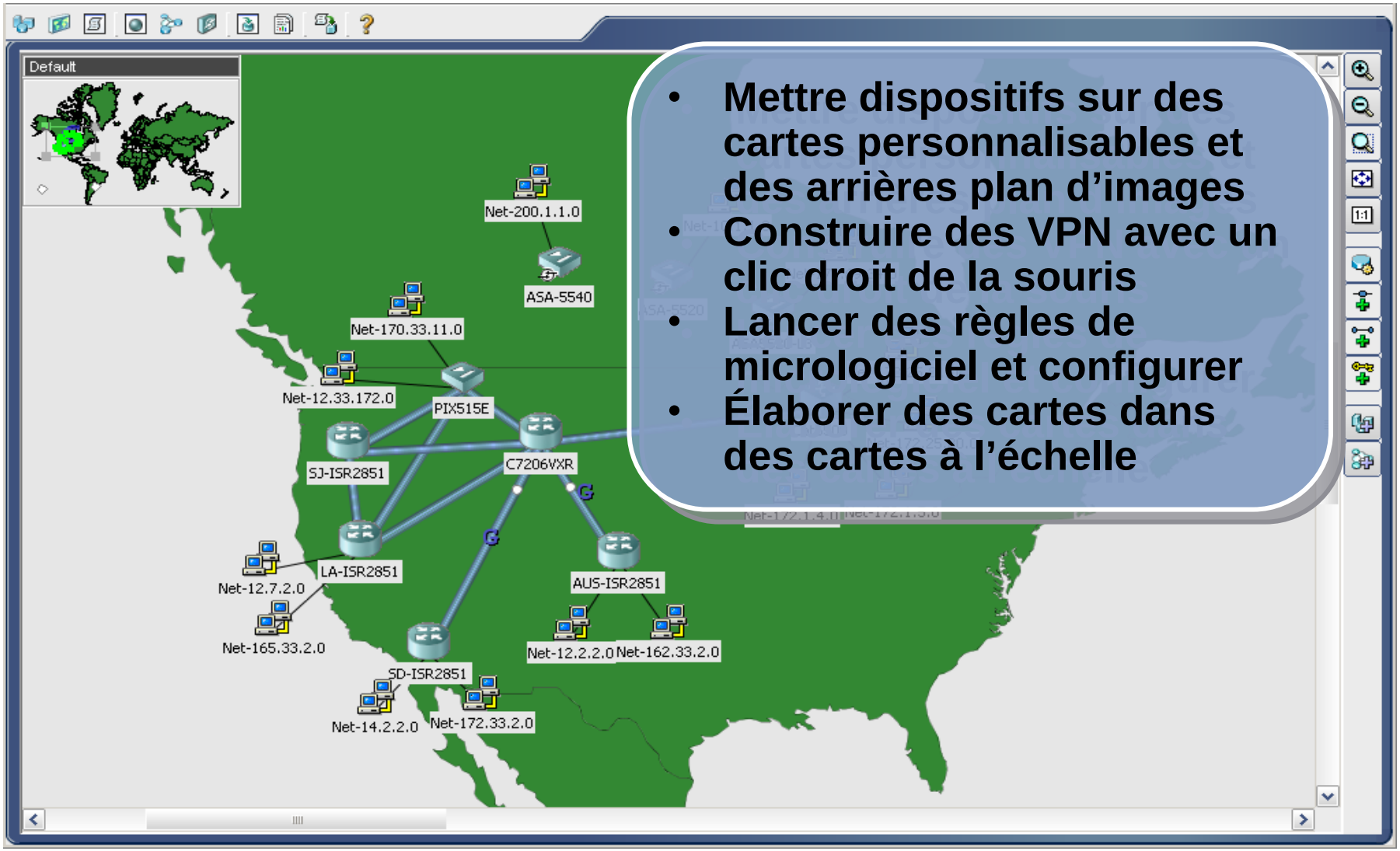
Vue centrée sur le dispositif



Vue basée sur les politiques

- **Gestion centralisée des politiques**
- **Extensibilité puissante via l'héritage, la réutilisation, l'attribution et le partage**

Vue centrée sur la topologie



- Mettre dispositifs sur des cartes personnalisables et des arrières plan d'images
- Construire des VPN avec un clic droit de la souris
- Lancer des règles de micrologiciel et configurer
- Élaborer des cartes dans des cartes à l'échelle

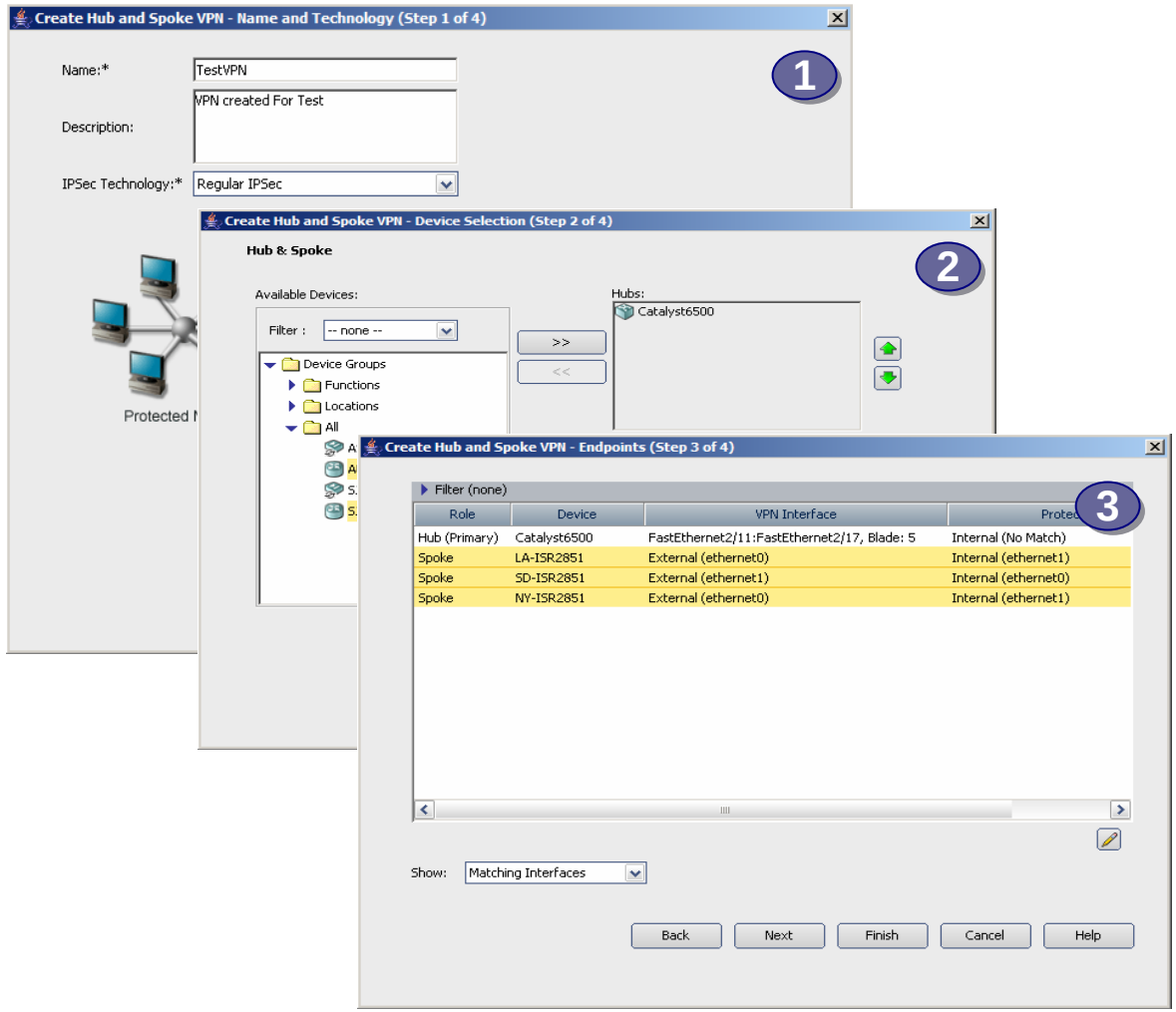
VPN – Configuration basée sur assistant

- Configuration basée sur assistant
- Trois étapes pour créer un VPN

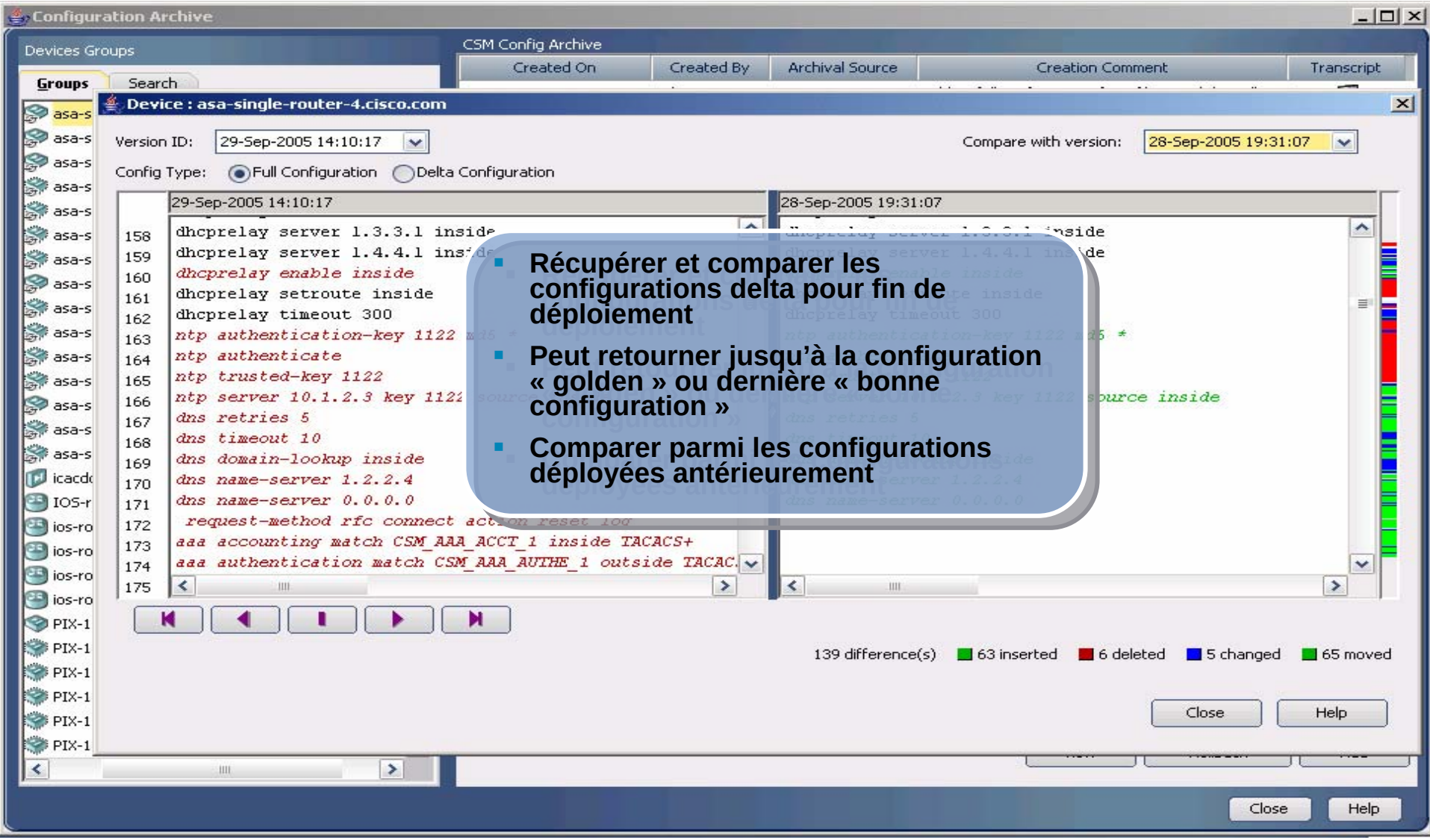
1 → Choisir la topologie VPN et la technologie.

2 → Choisir les participants.

3 → Personnaliser le trafic protégé s'il y a lieu.



Outils puissants : archive de configuration



- **Récupérer et comparer les configurations delta pour fin de déploiement**
- **Peut retourner jusqu'à la configuration « golden » ou dernière « bonne configuration »**
- **Comparer parmi les configurations déployées antérieurement**

Modèle de partage de politique et d'héritage
« Définition de politique extensible, configuration une fois et déploiement à plusieurs dispositifs »

Qu'est-ce que c'est?

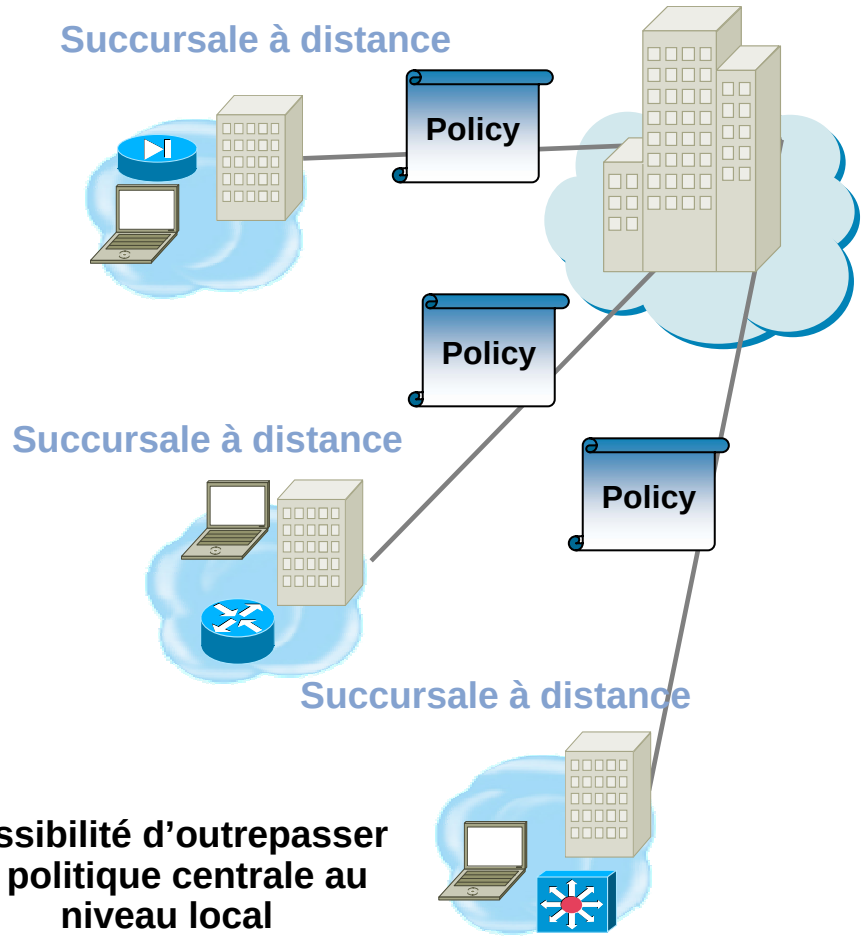
- Dispositif découplé forme les politiques

Exemple

- Partage de politiques communes sur les groupes de dispositifs pour
  - le pare-feu de la succursale
  - VPN site à site
  - Gestion de dispositifs
- Politiques d'entreprise obligatoires
  - Aucun trafic Napster, point
  - Permet SSH et SSL

Avantage

- Réduction de la complexité pour les administrateurs
- Effectuer plus de tâches avec moins de ressources



Possibilité d'outrepasser la politique centrale au niveau local

Renforcement de la politique basée sur les domaines
« Contrôle granulaire de quel trafic circule où »

Groupes d'interfaces

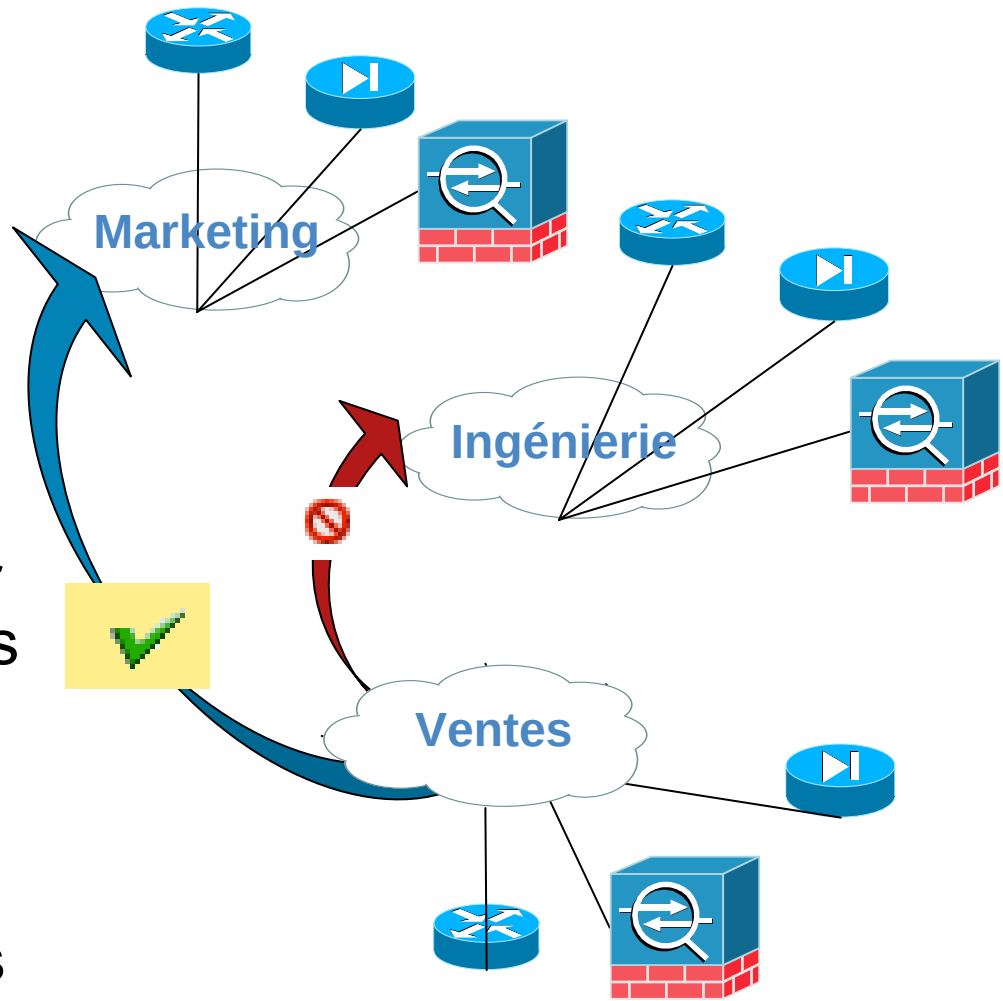
- Interfaces liées à un domaine
- Personnalisables par l'utilisateur

Exemple

- Définir les politiques pour contrôler le trafic entre les domaines

Avantage

- Renforcement des politiques en fonction des besoins organisationnels



Flux des travaux

« Permettre à différentes équipes de gestion de travailler ensemble »

Qu'est-ce que c'est?

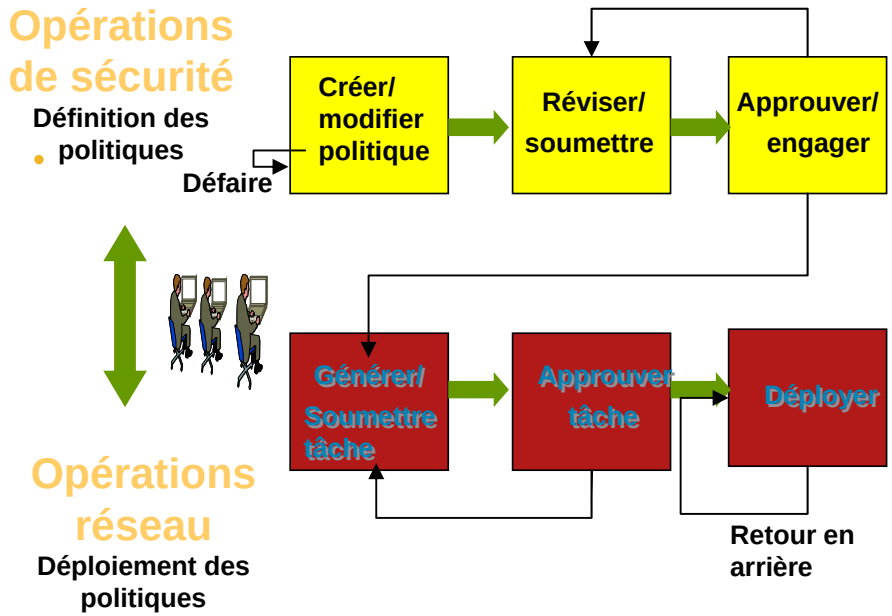
- Processus structuré pour la gestion du changement qui complète votre environnement d'exploitation

Exemple

- Qui établit les politiques
- Qui les approuve
- Qui peut approuver le déploiement et à quel moment
- Qui peut les déployer

Avantages

- Permet le travail d'équipe et la collaboration entre les opérations réseau et les opérations de sécurité
- Procure la portée du contrôle



Pare-feu, VPN et services IPS

Contrôle des accès basé sur les rôles

Qu'est-ce que c'est?

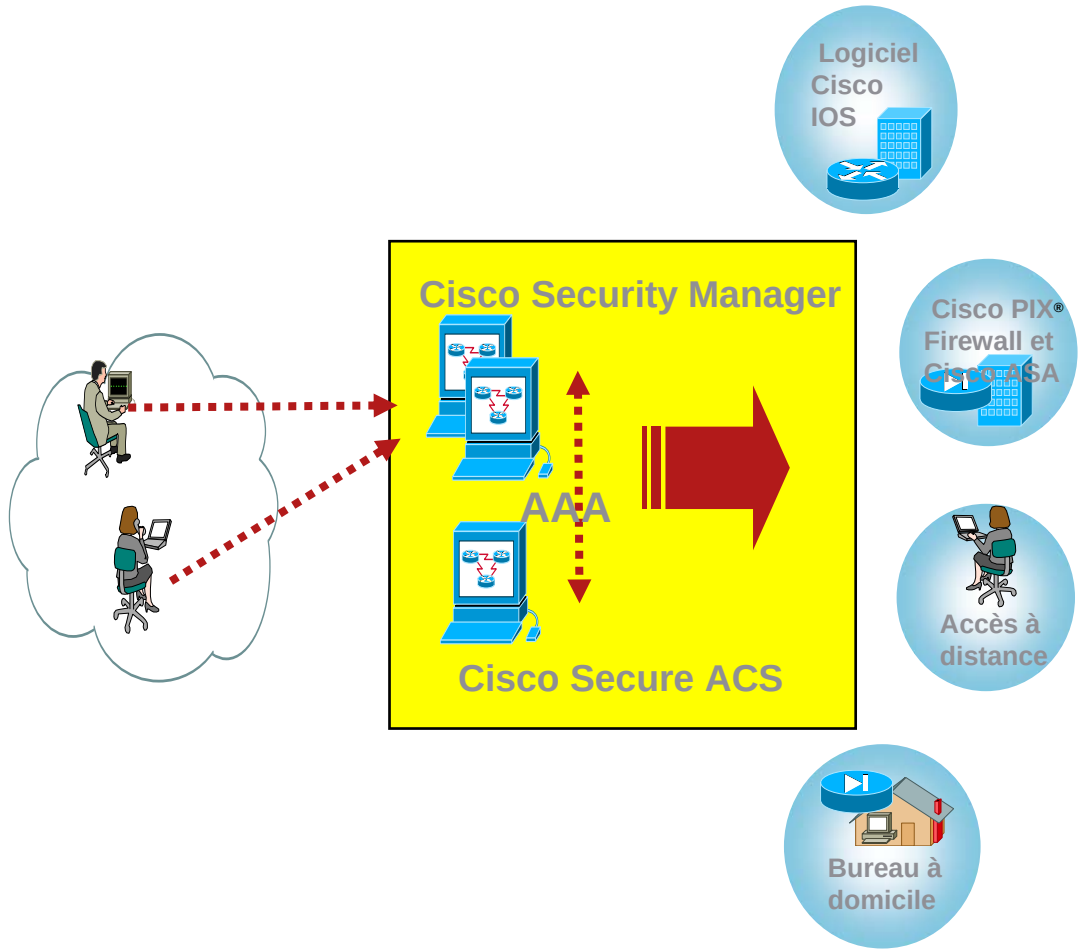
- **Authentifie l'accès de l'administrateur au système de gestion**
- **Détermine les utilisateurs qui ont accès à des dispositifs spécifiques et les fonctions de politiques**

Exemple

- **Vérifie l'administrateur et associe les administrateurs à des rôles spécifiques et détermine qui fait quoi**

Avantages

- **Permet de déléguer les tâches administratives à plusieurs opérateurs**
- **Procure la distinction appropriée de l'appartenance et des contrôles**



Déploiement réparti extensible

Qu'est-ce que c'est?

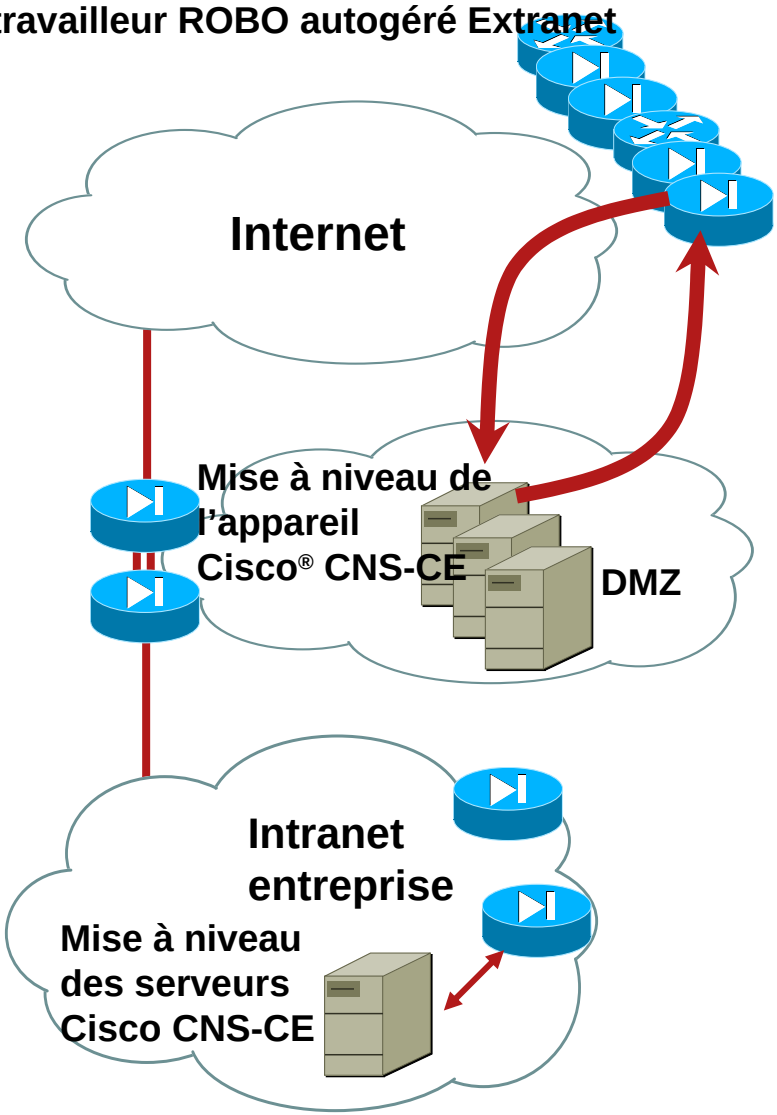
- Une méthode simplifiée du déploiement réparti pour des milliers de dispositifs à distance

Exemple

- Mises à jour d'un grand nombre de pare-feu à distance qui peuvent avoir des adresses dynamiques, des liens intermittents ou des adresses NAT
- Met à jour les configurations et les images logicielles
- Les dispositifs sont mis à jour eux-mêmes lorsqu'ils sont en ligne
- Extension à l'ensemble des technologies Web

Avantage

- Aide les clients qui comptent des milliers de télétravailleurs et d'établissements à distance et qui ont un effectif technique minimal dans un site à distance

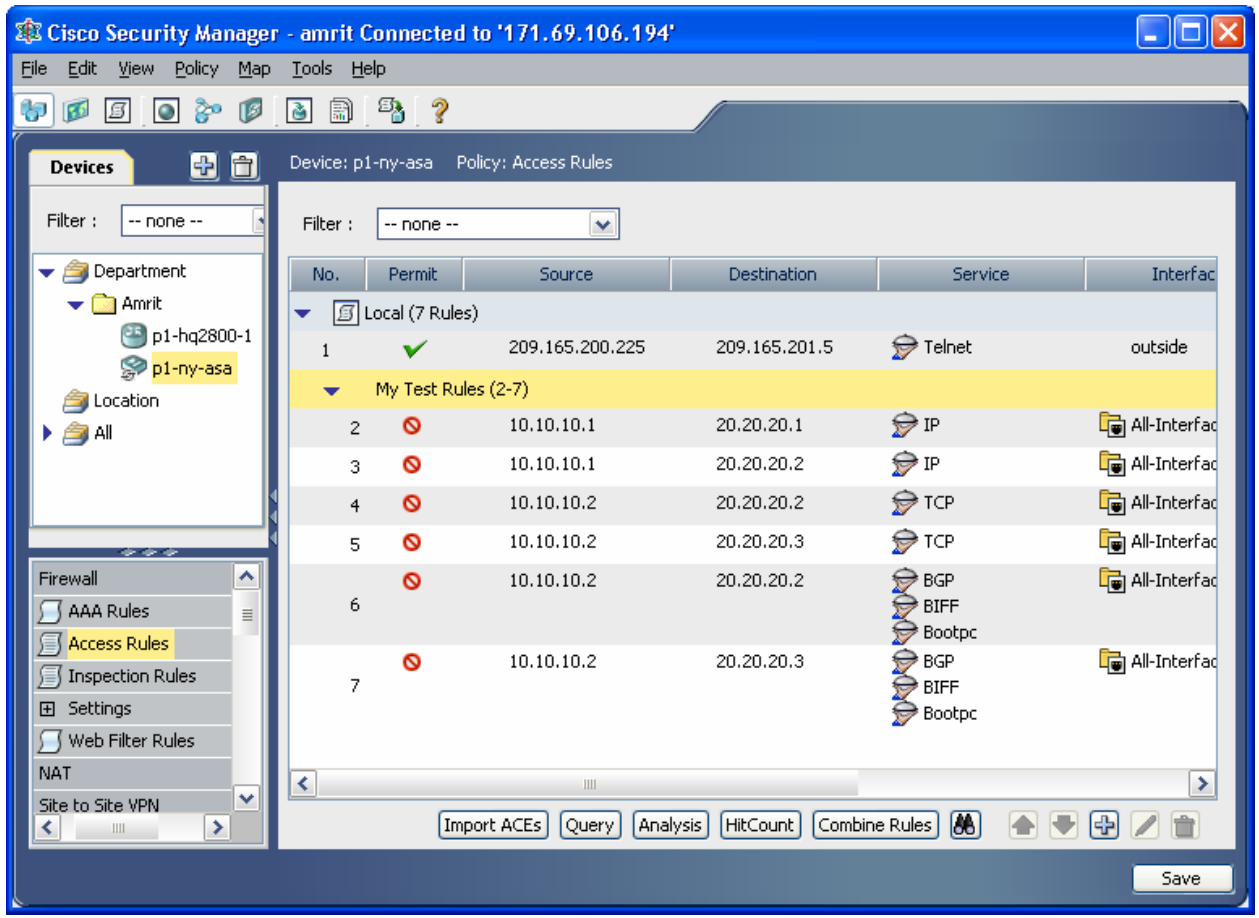


Cisco Security Manager 3.1 – Nouvelles fonctions

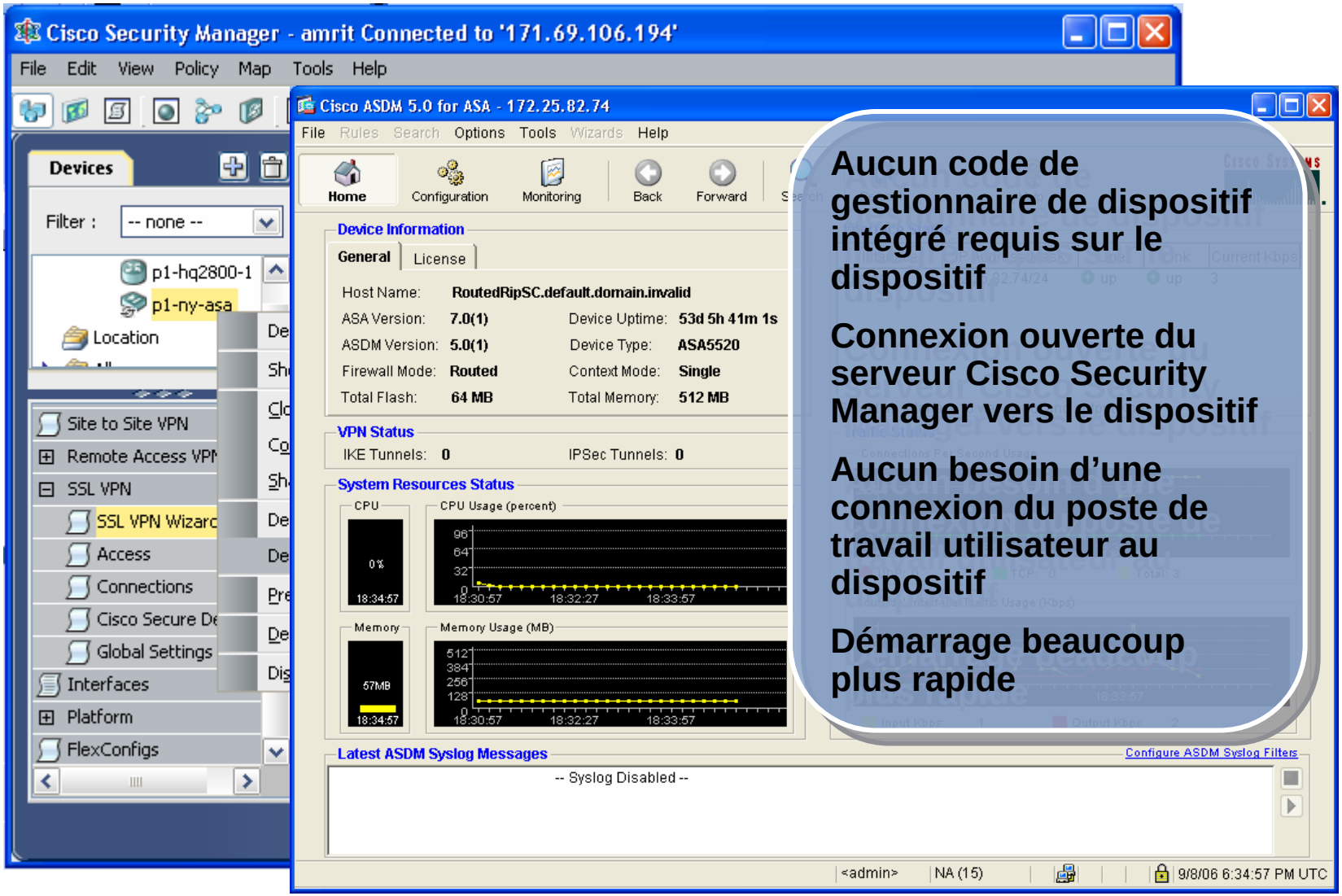
- **IPS natif**
- **Découverte VPN**
- **Support VPN SSL**
- **Amélioration à la table des règles, dossiers et règles locales**
- **Combinaison de règles**
- **Interface évoluée du logiciel Cisco IOS® et découverte des paramètres de plate-forme**
- **Lancement multi-plates-formes xDM (Cisco®ASDM, SDM, IDM et IEV)**
- **Cisco Catalyst® 6000 natif, RACL**
- **VACL sur Cisco Catalyst 6000**
- **Rapport d'inventaire avec état des dispositifs**
- **Test de connectivité du protocole de gestion**
- **Rapport détaillé des activités**

Cisco Security Manager 3.1
Règles locales et sections de table de règles

- Règles locales – Précisez facilement les règles locales outre les règles héritées.
- Sections de table des règles – Séparez la table des règles en sections.

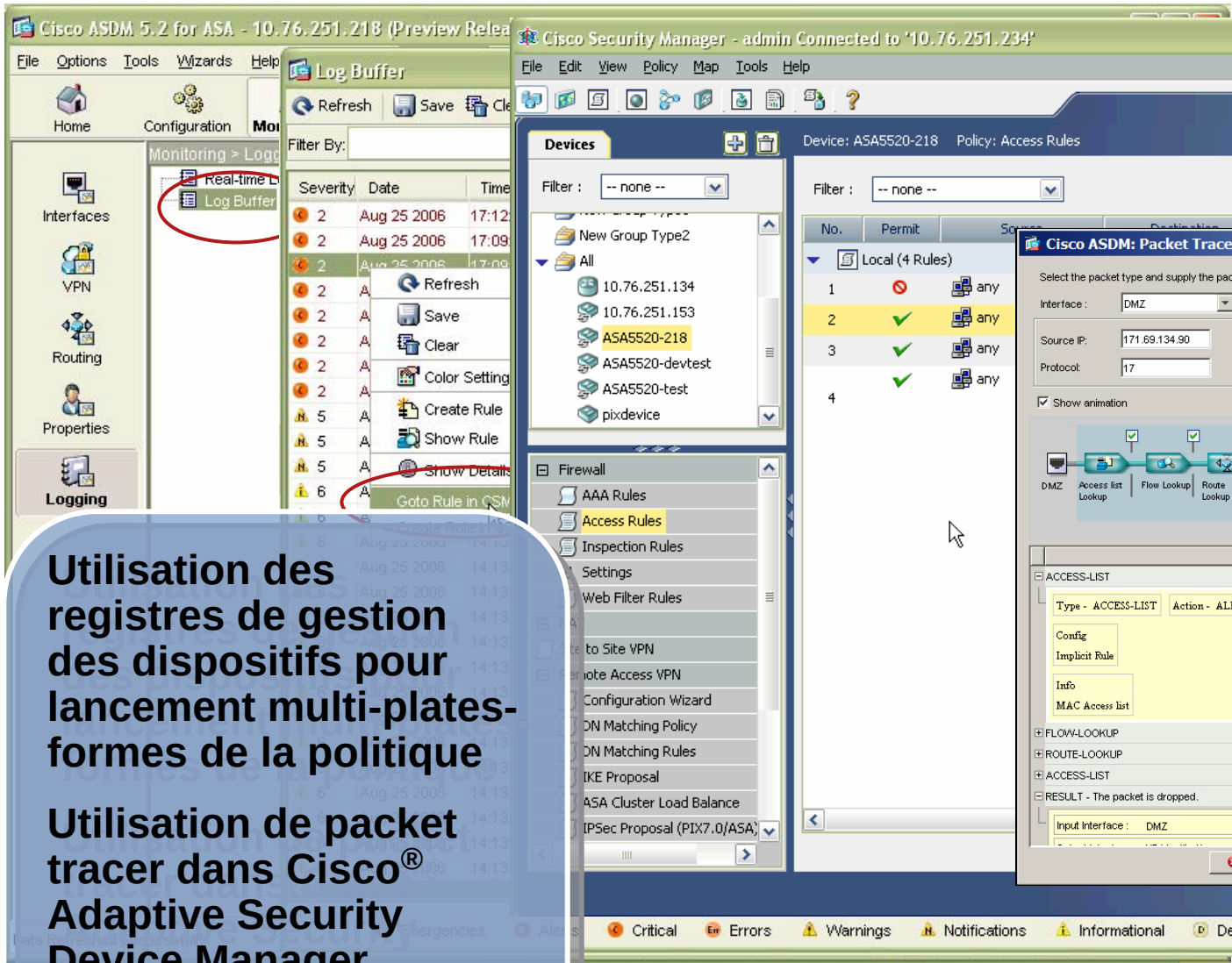


Cisco Security Manager 3.1 – Lancement multi-plate-forme xDM Cisco ASDM, SDM, IDM, and IEV



- Aucun code de gestionnaire de dispositif intégré requis sur le dispositif
- Connexion ouverte du serveur Cisco Security Manager vers le dispositif
- Aucun besoin d'une connexion du poste de travail utilisateur au dispositif
- Démarrage beaucoup plus rapide

Cisco Security Manager 3.1 – xDM

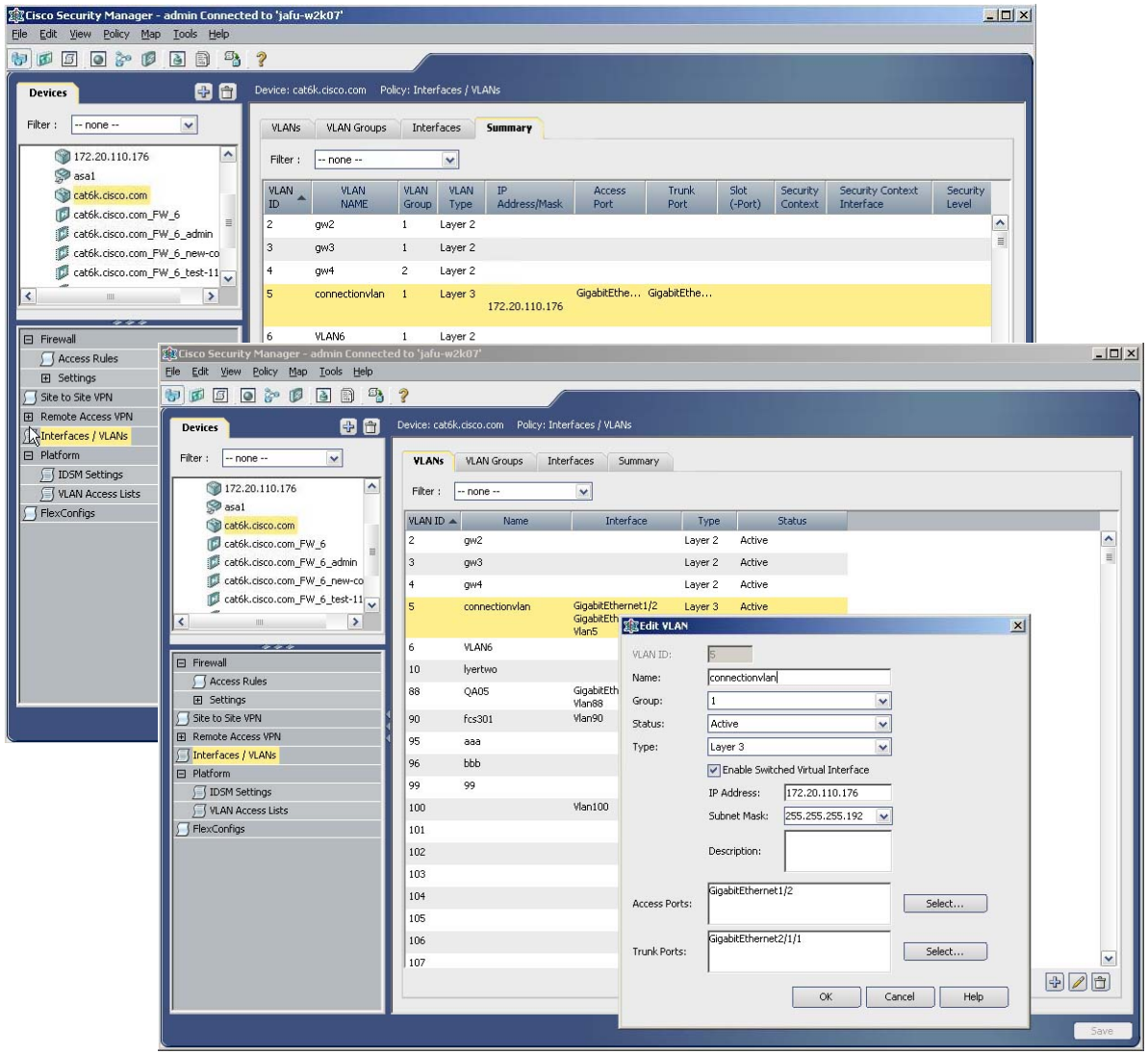


Utilisation des registres de gestion des dispositifs pour lancement multi-plates-formes de la politique

Utilisation de packet tracer dans Cisco® Adaptive Security Device Manager (ASDM)

Cisco Security Manager 3.1 – Gestion en mode natif de Cisco Catalyst 6000
Interfaces, VLANs et groupes VLAN

- Gestion en mode natif de Cisco Catalyst® 6500 et Cisco® 7600; plus besoin de lancer CiscoView Device Manager (CVDM).
- Gestion de tous les VLANs, interfaces, groupes VLAN et cartes.
- Page de sommaire détaillée indiquant tous les mappages.



Cisco Security Manager 3.1 –Rapport d'activité Champs modifiés; objets modifiés

Activity Change Report

User: admin
Session started on: 13-Nov-2006 13:46:01
Current state: Edit Open
Report created on: 13-Nov-2006 17:45:30

Devices

mypix.cisco.com

Access Rule

Access Rule

Operation	No.	Mandatory	Permit	Source	Destination	Service	Interface	Dir.	Category	Enabled
Add	1	true	permit	any,	any,	HTTP, HTTPS, FTP	All-Interfaces	in	None	true
Add	2	true	deny	any,	any,	IP	All-Interfaces	in	None	true

10.89.33.138

Device was discovered

Shared Policies

IPS-IpsEASetting

IpsEASetting: **10.89.33.138_IpsEASetting_1**
163454688687 (Added)

Inherits From	--None--
Affected Devices	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138
New Assignments	Total:2. Devices: 10.89.33.138_johnq-vs1 , 10.89.33.138

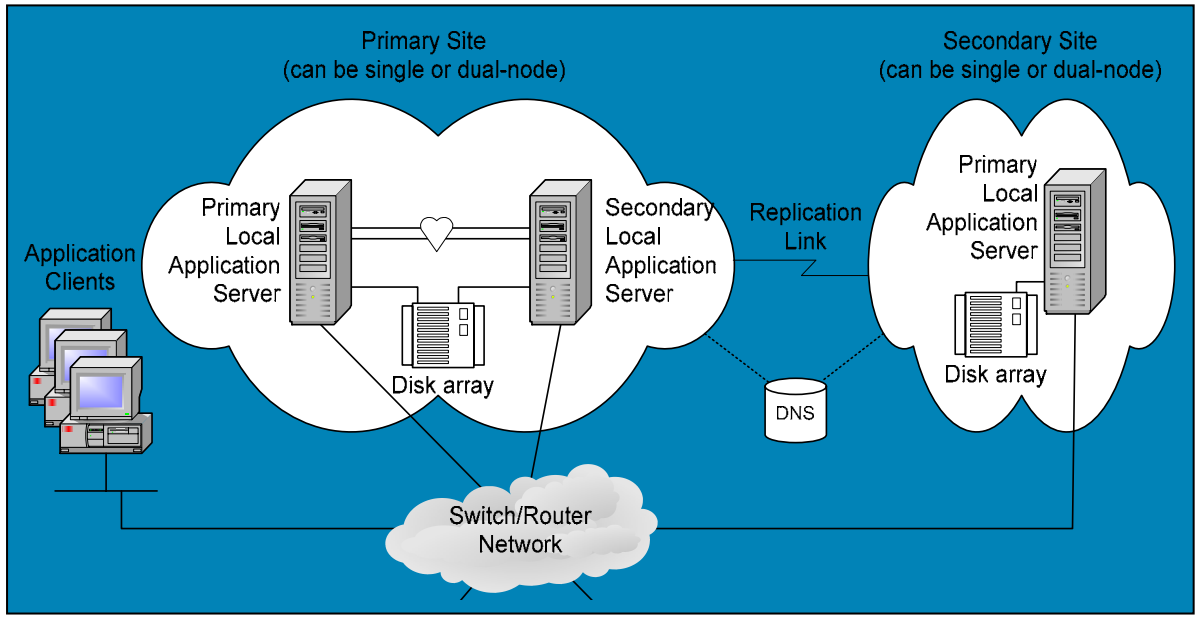
IpsEASetting

Operation	Global -deny -timeout
Add	3609

IPS-IpsAnomalyDetection

Cisco Security Manager 3.1
Grande disponibilité et reprise après sinistre

- Configuration optionnelle de haute disponibilité et de reprise après sinistre
- Matériel clé en main (serveurs, matrices de stockage) et (Symantec/Veritas) plus des personnalisations spécifiques pour Cisco® Security Manager

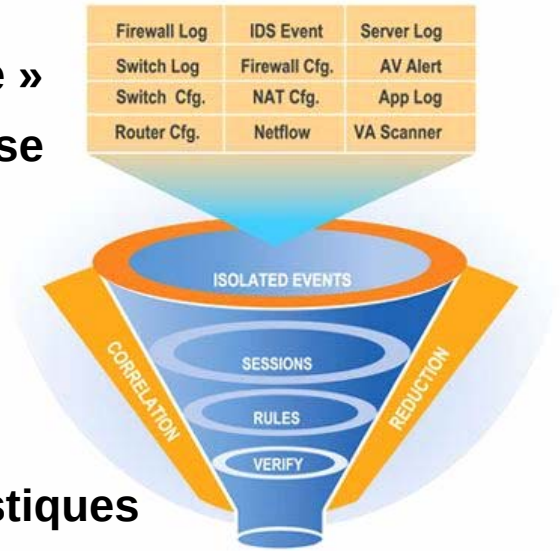


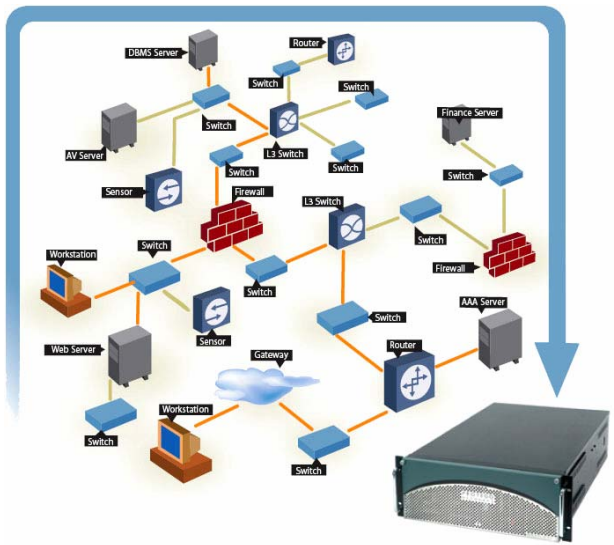
- Prend en charge une grande variété d'options de déploiement basées sur les exigences du client
  - Grappe double nœud unique pour grande disponibilité
  - Plusieurs grappes réparties géographiquement pour reprise après sinistre
  - Détection de panne et reprise entièrement automatisée
  - Stockage local partagé pour assurer qu'il n'y aura aucune perte de données
  - Duplication synchrone ou asynchrone entre les sites pour assurer aucune perte ou presque de données

Surveiller, Analyser et Réagir avec CS-MARS

Cisco Security – MARS
Monitoring, Analysis and Response System

- **Commande et contrôle de votre investissement existant pou construire une sécurité « omniprésente »**
- **Corrélation des données de l'ensemble de l'entreprise**
  - **NIDS, pare-feu, routeurs, commutateurs, CSA**
  - **Syslog, SNMP, RDEP, SDEE, NetFlow, registres d'évènements de dispositifs d'extrémités, multi-fournisseurs**
- **Localisation et atténuation rapides des attaques**





- **Principales caractéristiques**

  Détermine les *incidents* de sécurité en fonction des *messages*, *évènements* et *sessions* des dispositifs

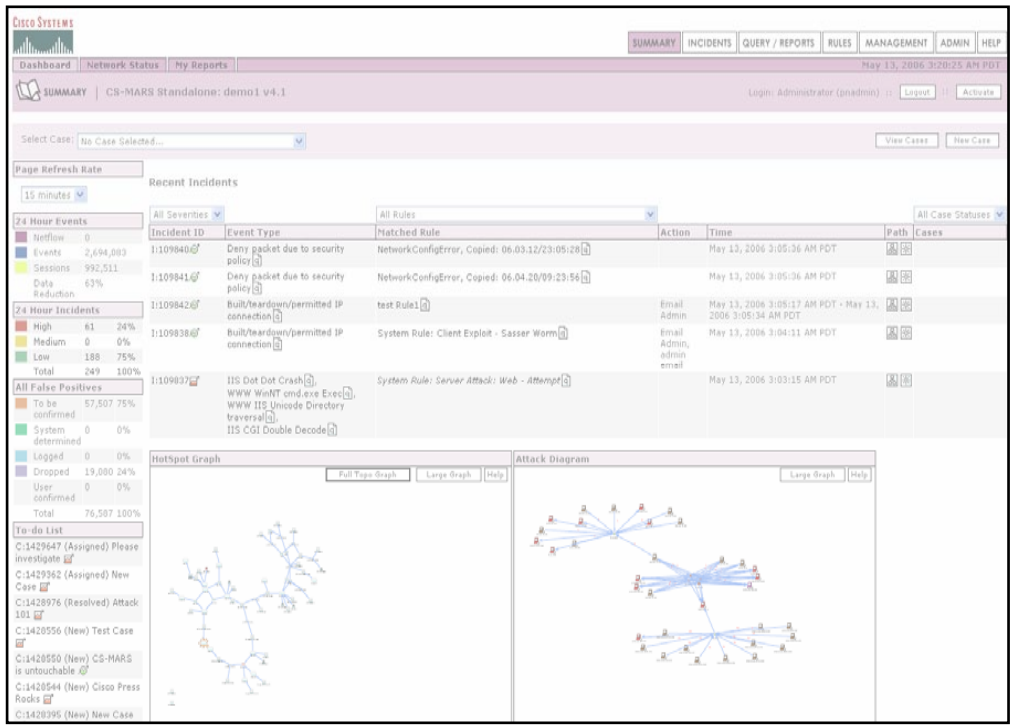
  Les *incidents* sont sensibles de façon topologique à la visualisation et reprise

  Atténuation sur les ports de couche 2 et de point d'engorgement de couche 3

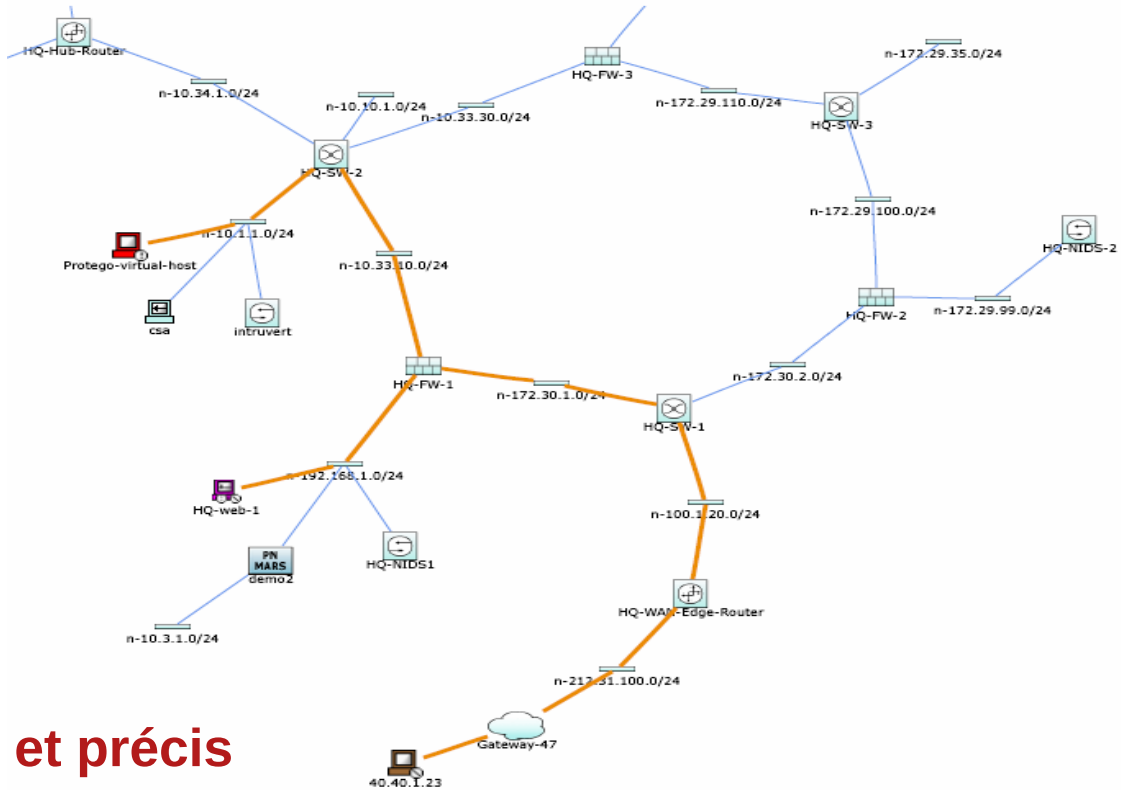
Vue d'ensemble du centre de Commande/ Contrôle

- Utilisation de Netflow, Syslog et la topologie de dispositif sont comme entrées

MARS devient le centre de commande et de contrôle



Sensibilisation de l’attaque au niveau de la topologies



Analyse SureVector

- **Chemin de l’attaque visible et précis**
- **Détails complets de l’incident et de l’évènement brut**
- **Cibler la véritable source d’anomalies et de comportement de l’attaque**
- **Situation plus complète et exacte**

Commande et contrôle : atténuation de l'attaque

- **Utiliser les fonctionnalités de contrôle de votre infrastructure**
  - **Chemin de l'attaque couches 2/3 est très visible**
  - **Dispositifs de renforcement de l'atténuation sont identifiés**
  - **La commande exacte d'atténuation est fournie**

Enforcement Device: **switch_server**, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch-IOS 12.2	Protego Networks MARS 1.0 on pnvalis		N/A		

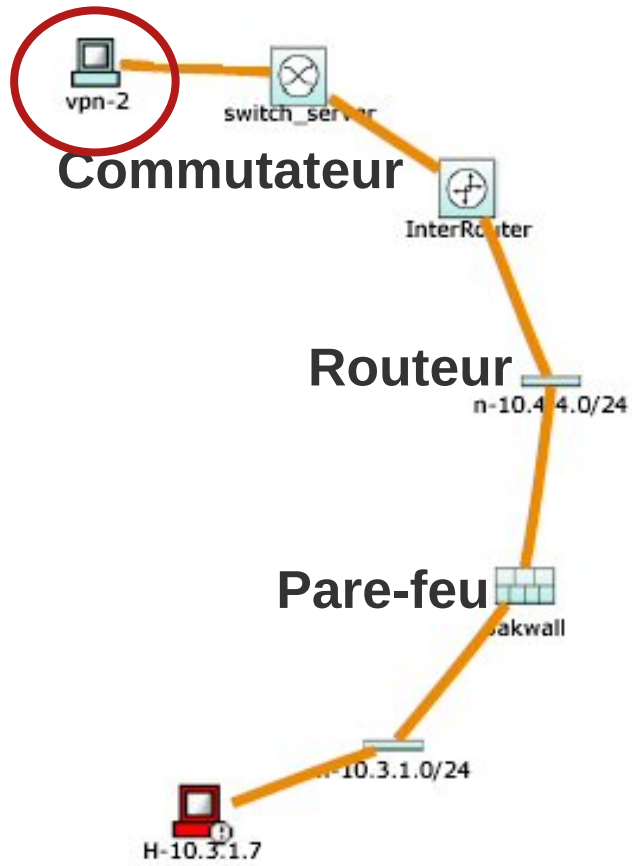
Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time

Recommended Policy/Command

```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```

Push Cancel



CS-MARS – Équipements Supportés

- **Networking**
  - Cisco IOS® 11.x and 12.x Software, Cisco Catalyst® OS 6.x
  - NetFlow v1/v5/v7
  - NAC ACS 3.x, 4.x
  - Extreme Extremeware 6.x
- **Firewall/VPN**
  - Cisco® PIX® 6.x, 7.x Firewall, ASA, Cisco IOS Firewall/IPS, FWSM 1.x, 2.x, 3.1, VPN Concentrator 4.x
  - CheckPoint Firewall-1 NG FPx, NG AI, NGX AI, VPN-1
  - NetScreen Firewall 4.x, 5.x
  - Nokia Firewall
- **IDS**
  - Cisco NIDS 4.x, 5.x, IDSM 4.x, 5.x
  - Cisco ICS
  - Enterasys Dragon NIDS 6.x
  - ISS RealSecure Network Sensor 6.5, 7.0
  - Snort NIDS 2.x
  - McAfee Intrushield NIDS 1.x
  - NetScreen IDP 2.x
  - Symantec ManHunt 3.x
- **Vulnerability Assessment**
  - eEye REM 1.x
  - Foundstone FoundScan 3.x
  - QualysGuard 3.3
- **Host Security**
  - Cisco Security Agent (CSA) 4.5
  - McAfee Entercept 2.5, 4.x
  - McAfee ePO
  - ISS RealSecure Host Sensor 6.5, 7.0
  - Symantec AnitVirus 9.x
- **Host Log**
  - Windows NT, 2000, 2003 (agent/agent-less)
  - Solaris
  - Linux
- **Syslog**
  - Universal device support
- **Applications**
  - Web servers (IIS, iPlanet, Apache)
  - Oracle 9i, 10i database audit logs
  - Network Appliance NetCache

Établissement de rapports

Rapports de conformité

Rapports populaires avec options de personnalisation et de distribution

Les interrogations sont sauvegardées comme des règles ou des rapports — cadre de travail intuitif

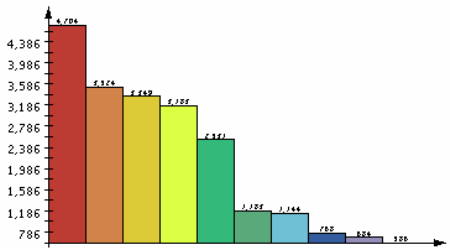
Report: Activity: Denies - Top Destination [illegible] 1:07:45 PM PDT

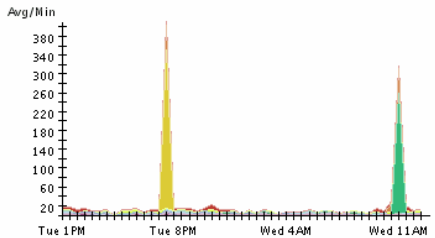
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

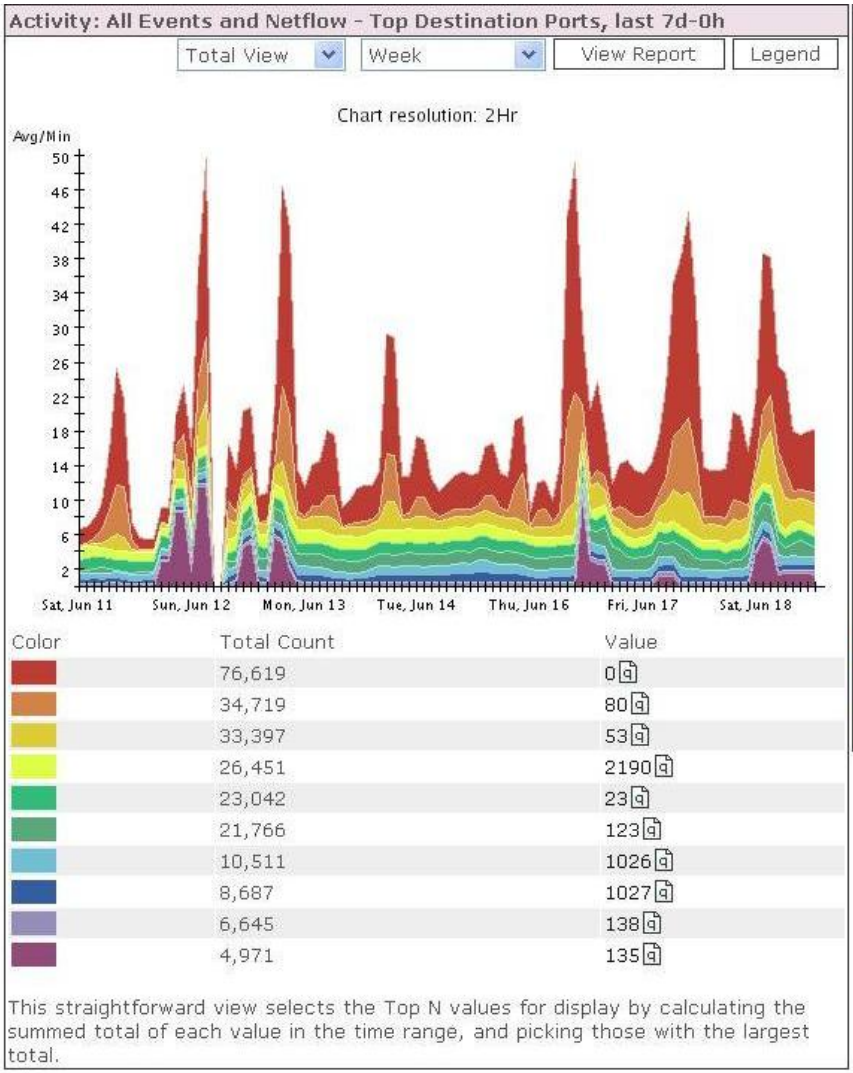
Keywords: [None]

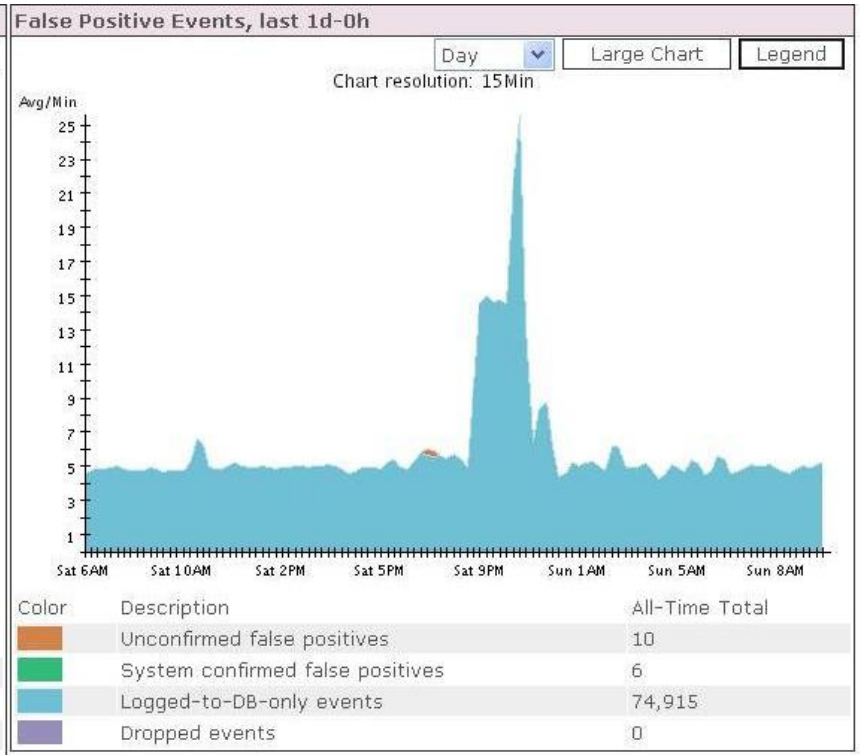




Rank		Count (# of sessions)	Raw Destination Port
	1	4704	445
	2	3524	80
	3	3349	26686
	4	3183	135
	5	2531	47683
	6	1183	1026
	7	1144	0
	8	768	139
	9	684	9898

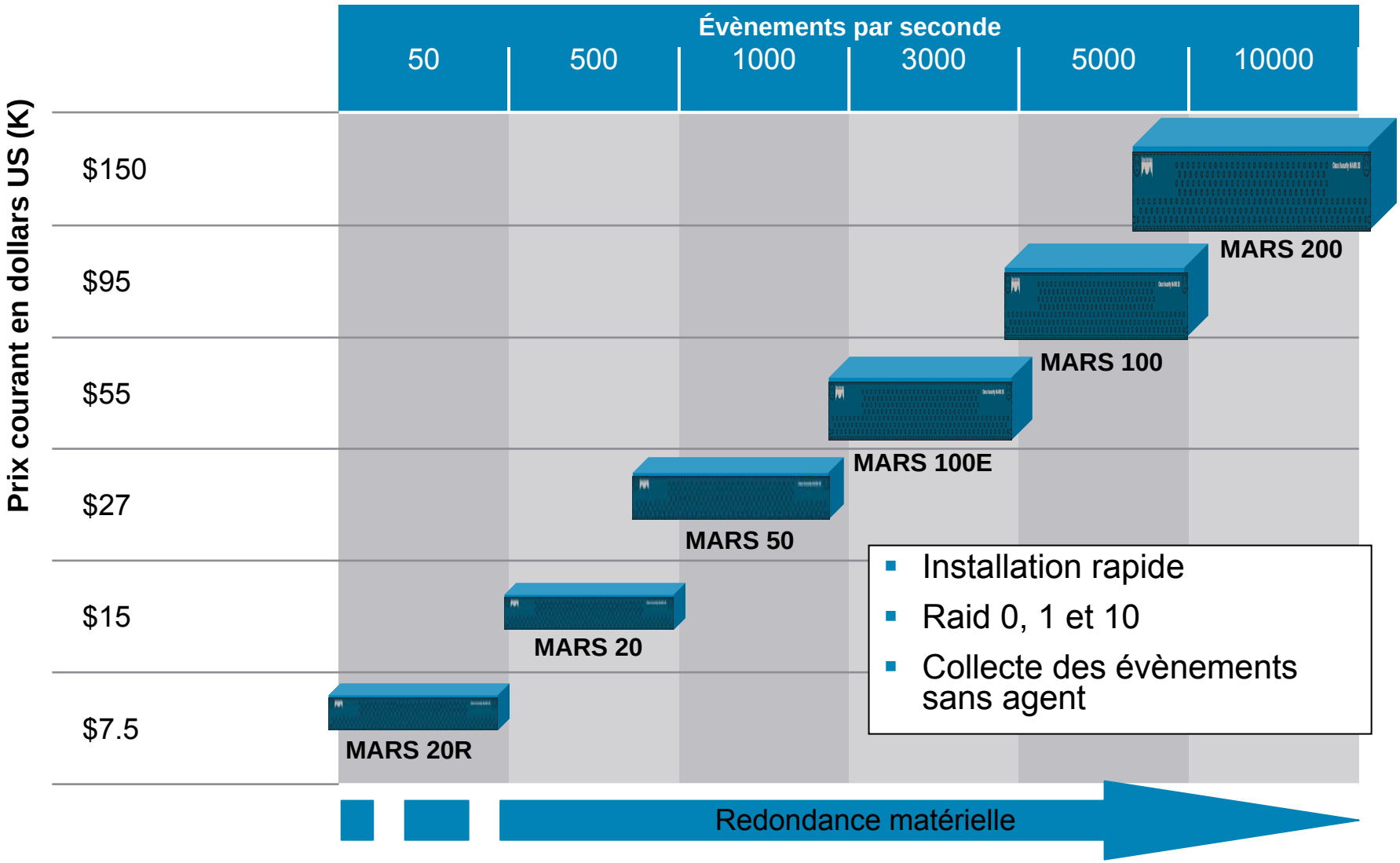
Examen du trafic du réseau



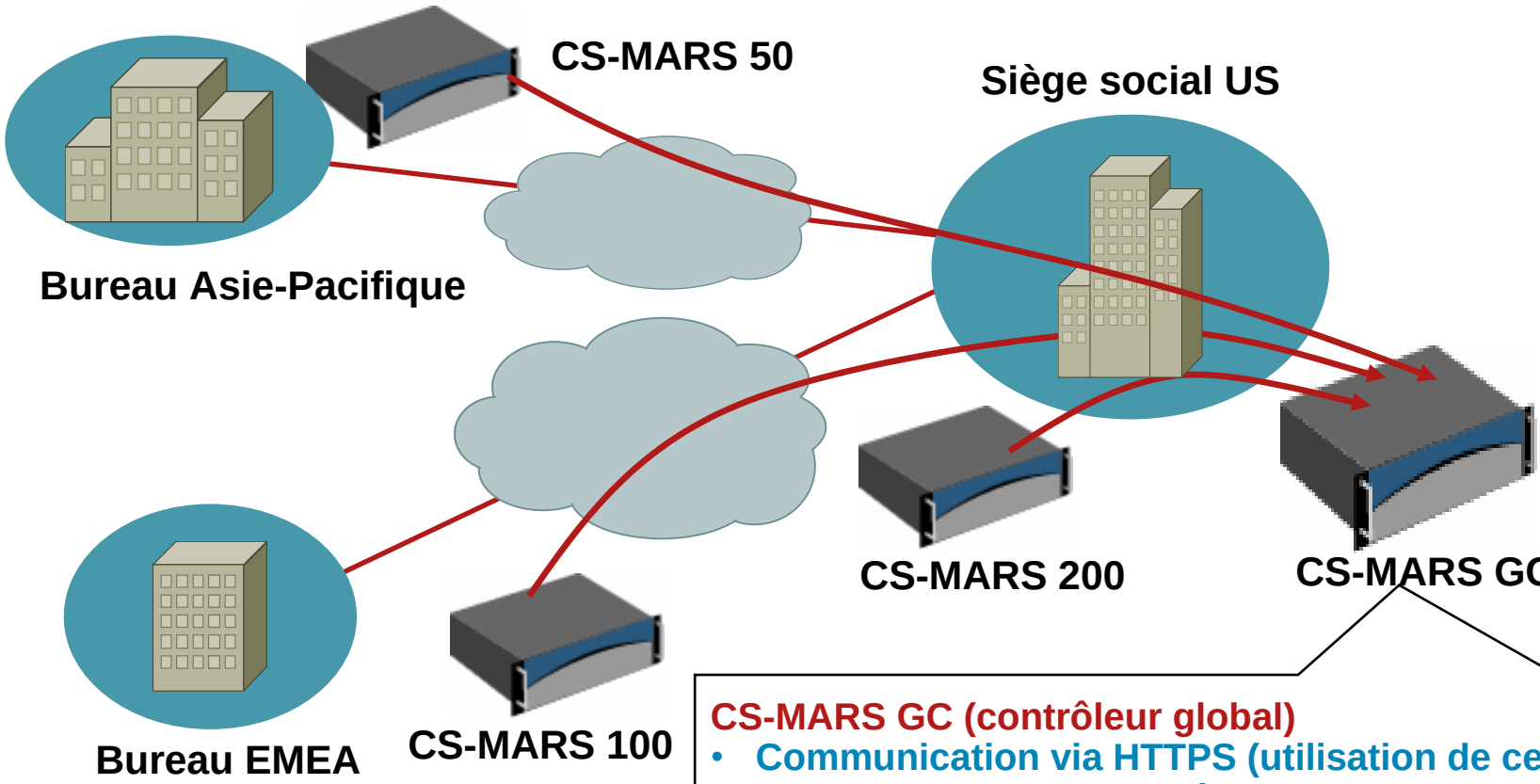


Appareils CS-MARS

Survol de l'appareil CS-MARS



Déploiement CS-MARS



CS-MARS GC (contrôleur global)

- Communication via HTTPS (utilisation de certificats)
- Seuls les incidents des règles globales sont déployés
- Le contrôleur global distribue les mises à jour, règles, gabarits de rapports, règles d'accès et interrogations sur le LC

Versions MARS à venir (2007)

Version 4.3/5.3 (1H 2007)
Principaux avantages

- **Élargissement des modèles de stockage**
  - Nouveau matériel pour modèles 110R et modèles ultérieurs, extension du stockage 2x
- **Modèles à performance améliorée**
  - Nouveau matériel pour modèles 110R et ultérieurs, performance améliorée 1.5x
- **Signatures mises à jour**
  - Mises à jour de signature des dispositifs Cisco et non Cisco

Sommaire CS-MARS

Meilleur

Intelligence réseau intégré

Isoler l'attaquant par MAC, port de commutation

Stopper les attaques en cours

Visualiser le chemin de l'attaque

Renforcement de la sécurité du système d'exploitation et du système

Plus rapide

Analyse des évènements en mémoire

Algorithmes en attente de brevets

10 000 EPS avec corrélation complète (3-10x competition)

Architecture d'analyse des évènements extensibles et répartis avec CS-MARS Global Controller

Moins dispendieux

Offre groupée de l'appareil

Aucun coût caché pour logiciel/personnalisation

Licence simple – aucun agent de logiciel

Démonstration

Cisco Self-Defending Network